



Guide de GuardDuty l'utilisateur Amazon

Amazon GuardDuty



Amazon GuardDuty: Guide de GuardDuty l'utilisateur Amazon

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 que c'est GuardDuty ?	1
Caractéristiques de GuardDuty	2
Conformité PCI DSS	8
Tarification en GuardDuty	8
Utilisation de l' GuardDuty essai gratuit de 30 jours	9
Utilisation de la protection contre les programmes malveillants pour S3 avec le niveau gratuit	11
Accès GuardDuty	11
Concepts et termes clés	13
Prise en main	19
Avant de commencer	19
Étape 1 : activer Amazon GuardDuty	22
Étape 2 : générer des exemples de résultats et explorer les opérations de base	24
Étape 3 : configurer l'exportation GuardDuty des résultats vers un compartiment Amazon S3	25
Étape 4 : configurer les alertes de GuardDuty recherche via SNS	31
Étapes suivantes	34
Source de données de base	36
AWS CloudTrail événements de gestion	36
Comment GuardDuty gère AWS CloudTrail événements mondiaux	37
Journaux de flux VPC	38
Journaux de requêtes DNS de Route53 Resolver	39
Détection étendue des menaces	40
Exemples de scénarios de menace liés à une séquence d'attaques	40
Comment fonctionne la détection étendue des menaces	41
Mettre en place des plans de protection pour optimiser la détection des menaces	43
Détection de séquences d'attaques dans les clusters Amazon EKS	43
Détection de séquences d'attaques dans les compartiments Amazon S3	45
Détection de séquences d'attaques dans les clusters Amazon ECS	45
Détection de séquences d'attaque dans les groupes d'instances Amazon EC2	46
Détection de séquences d'attaques impliquant des charges de travail basées sur l'IA	47
Détection étendue des menaces dans GuardDuty la console	47
Comprendre et gérer les résultats des séquences d'attaques	48
Ressources supplémentaires	48
Plans de protection	50

Présentation de	50
Configuration de tous les plans de protection	51
Auto-enable options	51
Configuration de la surveillance de l'exécution	52
Contraintes bidirectionnelles	52
Statistiques de l'organisation	53
Intégration de la page des comptes	54
Protection de l'IA	55
Comment fonctionne la protection par IA	56
Tarification de la protection de l'IA	57
Détections de menaces supplémentaires pour les charges de travail liées à l'IA	58
Activation de la protection par l'IA dans les environnements à comptes multiples	59
Activation de la protection par l'IA pour un compte autonome	63
Protection EKS	65
Journaux d'audit EKS dans EKS Protection	66
Activation de la protection EKS dans les environnements à comptes multiples	67
Activation de la protection EKS pour un compte autonome	74
Protection S3	76
AWS CloudTrail événements de données pour S3	77
Comment GuardDuty utilise les événements de CloudTrail données pour S3	77
GuardDuty utilisation d'événements de CloudTrail données pour S3 pour les séquences d'attaque	78
Activation de la protection S3 dans les environnements à comptes multiples	79
Activation de S3 Protection pour un compte autonome	86
Surveillance d'exécution	88
Comment ça marche	89
Habilitation	90
Déploiement sur Amazon EKS	91
Déploiement sur Amazon EC2	93
Déploiement sur Amazon ECS sur Fargate	95
Connectivité des agents	96
Suivi du temps d'exécution Surveillance de la couverture	98
essai gratuit de 30 jours	99
J'utilise la période GuardDuty d'essai ou je n'ai jamais activé EKS Runtime Monitoring	99
J'ai activé EKS Runtime Monitoring avant le lancement de Runtime Monitoring	100
Conditions préalables	101

Pour l'instance EC2	101
Pour ECS-EC2 Bottlerocket	105
Pour le cluster Fargate (ECS uniquement)	109
Pour le cluster EKS	116
Architectures de processeur, systèmes d'exploitation et versions de noyau pris en charge ..	119
Activer la surveillance du temps d'exécution	121
Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples	121
Activation de la surveillance du temps d'exécution pour un compte autonome	124
Gestion des agents GuardDuty de sécurité	125
Agent automatisé sur la ressource Amazon EC2	126
Gestion manuelle des agents pour les ressources Amazon EC2	139
Agent automatisé sur la ressource ECS-EC2 Bottlerocket	156
Agent automatisé sur la ressource Fargate (Amazon ECS uniquement)	157
Agent automatisé sur la ressource Amazon EKS	193
Gestion manuelle des agents pour le cluster Amazon EKS	231
Configuration des paramètres du module complémentaire EKS	240
Validation de la configuration des points de terminaison VPC	244
Problèmes de couverture du temps d'exécution et résolution des problèmes	245
Couverture et résolution des problèmes pour les ressources Amazon EC2	246
Couverture et résolution des problèmes pour ECS-EC2 Bottlerocket	264
Couverture et résolution des problèmes pour les clusters Amazon ECS	272
Couverture et résolution des problèmes pour les clusters Amazon EKS	289
Configuration de la surveillance du processeur et de la mémoire	305
Utilisation d'un VPC partagé	306
Comment ça marche	307
Conditions préalables	309
Utilisation d'iAc avec des agents automatisés	310
Présentation du graphe de dépendance des ressources laC	310
Problème courant : suppression de ressources dans laC	311
Types d'événement d'exécution collectés	312
Événements de processus	313
Événements de conteneur	315
AWS Fargate événements de tâches (Amazon ECS uniquement)	316
Événements du pod Kubernetes	317
Événements du système de noms de domaine (DNS)	317

Événements ouverts	318
Événement du module de charge	318
Événements Mprotect	319
Événements de montage	319
Événements du lien	320
Événements Symlink	320
Événements Dup	320
Événement de mappage de mémoire	321
Événements de socket	322
Événements de connexion	322
Événements Process VM Readv	323
Événements Process VM Writev	324
Événements de suivi des processus (Ptrace)	324
Lier des événements	325
Écoutez les événements	325
Renommer les événements	326
Définir les événements d'ID utilisateur (UID)	326
Événements Chmod	327
Agent d'hébergement GuardDuty de référentiels Amazon ECR	327
Dépôt ECR pour EKS v1.16.0 - 1.8.1 (eks.build.2)	328
Dépôt ECR pour la version EKS 1.8.1.eks.build.1	333
Référentiel ECR pour l'agent de sécurité activé AWS Fargate (Amazon ECS uniquement) ..	335
Référentiel ECR pour l'agent de sécurité sur ECS-EC2 Bottlerocket	339
Agents de sécurité sur le même hôte	343
Vue d'ensemble	344
Impact	344
Comment GuardDuty gère plusieurs agents	344
Surveillance d'exécution EKS	345
Configuration de la surveillance du temps d'exécution EKS pour les environnements à comptes multiples (API)	346
Configuration de la surveillance du temps d'exécution EKS pour un compte autonome (API)	388
Migration de la surveillance d'exécution EKS vers la surveillance d'exécution	396
GuardDuty versions publiées de l'agent de sécurité	400
Ressources supplémentaires - prochaines étapes	444
Désactivation, désinstallation et nettoyage des ressources	444

Désinstallation manuelle de l'agent de sécurité pour les ressources Amazon EC2	446
Désinstaller les ressources de l'agent de sécurité pour ECS-EC2 Bottlerocket	448
Nettoyer les ressources des agents de sécurité	449
Protection contre les logiciels malveillants pour EC2	451
Comparaison entre l'analyse des GuardDuty-initiated programmes malveillants et l'analyse des On-demand programmes malveillants	452
Comment GuardDuty analyse les volumes EBS pour détecter les malwares	455
Volumes EBS pris en charge	457
Modifier l'ID de clé KMS par défaut	458
Configuration de la conservation des instantanés et de la couverture de numérisation EC2	459
Conservation des instantanés	459
Options d'analyse avec balises définies par l'utilisateur	461
Balise GuardDutyExcluded globale	465
GuardDuty-initiated analyse des logiciels malveillants	466
essai gratuit de 30 jours	468
Activation de l'analyse des GuardDuty-initiated programmes malveillants dans les environnements à comptes multiples	468
Activation de l'analyse des GuardDuty-initiated programmes malveillants pour un compte autonome	480
Résultats qui invoquent une analyse des GuardDuty-initiated logiciels malveillants	481
On-demand analyse des logiciels malveillants	484
Fonctionnement de l'analyse des On-demand logiciels malveillants	485
Lancer l'analyse des On-demand logiciels malveillants	486
Re-scanning instance Amazon EC2 précédemment scannée	489
Surveillance de l'état et des résultats de l'analyse des logiciels malveillants	489
GuardDuty compte de service	491
Quotas dans la protection contre les programmes malveillants pour EC2	494
Protection contre les logiciels malveillants pour S3	499
Tarification et coût d'utilisation	501
Révision des coûts d'utilisation	503
Comment ça marche	503
Présentation de	503
Autorisations de rôle IAM	503
Marquage facultatif des objets en fonction du résultat de l'analyse	504
Procédure après avoir activé la protection contre les programmes malveillants pour S3 pour un compartiment	504

Fonctionnalités de protection contre les malwares pour S3	507
(Facultatif) Commencez avec Malware Protection pour S3 uniquement (console)	508
Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket ..	510
Activation de la protection contre les programmes malveillants pour la détection des menaces S3 pour votre compartiment	510
Autorisations de rôle IAM	518
Résolution d'une erreur d'autorisation de rôle IAM	523
Étapes à suivre après avoir activé la protection contre les programmes malveillants pour S3 ...	524
On-demand Analyse des malwares S3	525
Conditions préalables	526
Lancer une analyse des programmes malveillants à la	526
Utilisation du contrôle d'accès basé sur des balises (TBAC)	527
Ajouter le TBAC à la ressource du compartiment S3	528
Afficher et comprendre l'état du compartiment protégé	530
Surveillance des scans d'objets S3	531
État du scan potentiel de l'objet S3 et état des résultats	532
Utilisation d'Amazon EventBridge	536
Utilisation des balises d'objets S3	546
Utilisation d' CloudWatch alarmes et de métriques	547
Résolution des problèmes	551
Résolution des problèmes liés à l'état du plan de protection	551
Résolution des problèmes liés au scan des programmes malveillants	555
Modification du plan de protection contre les programmes malveillants pour un compartiment protégé	555
Désactivation de la protection contre les programmes malveillants pour S3 pour un compartiment protégé	558
Supportabilité des fonctionnalités d'Amazon S3	559
Protection contre les programmes malveillants pour les quotas S3	568
Protection contre les logiciels malveillants pour AWS Backup	572
Vue d'ensemble	572
Comment ça marche	575
Vue d'ensemble	572
Rôle IAM requis pour la numérisation	577
Examen de l'état et du résultat de l'analyse des ressources	577
Révision des résultats générés	578
Autorisations relatives aux rôles IAM	579

Rôle du client fourni pour l'analyse des programmes malveillants	579
Informations sur les autorisations	579
Sécuriser le rôle	580
Comment GuardDuty Malware Protection utilise les subventions dans AWS KMS	580
GuardDuty Contexte de chiffrement de la protection contre les	581
Autorisations et politique de confiance pour le rôle	582
Commencez de manière autonome	586
Étapes pour démarrer avec Malware Protection for Backup	586
Lancer des scans à la demande	587
Console	587
API/CLI	588
Surveillance de l'état et des résultats de l'analyse des logiciels malveillants	588
Protection contre les malwares pour les quotas de sauvegarde	597
Protection RDS	601
Bases de données prises en charge	603
Activité de connexion RDS	605
Activité des données RDS	605
Activation de la protection RDS dans les environnements à comptes multiples	606
Activation de la protection RDS pour un compte autonome	615
Résolution des problèmes de surveillance de RDS Protection	616
Stockage RDS complet	617
Versions non prises en charge sur la base de données principale pour RDS pour PostgreSQL	617
Considérations supplémentaires en matière de sécurité	618
Protection Lambda	619
Surveillance de l'activité du réseau Lambda	620
Activation de la protection Lambda dans les environnements à comptes multiples	620
Activation de la protection Lambda pour un compte autonome	628
Enquête - Aperçu	630
Types d'analyses	630
Cross-Region inférence	631
Conditions préalables	632
Modèle d'accès pour les comptes d'administrateur et de membre	633
Création d'une enquête	634
Affichage des résultats de l'enquête	637
Interpréter les résultats des enquêtes	638

Enquêtes sur les listes	639
Règles de détection personnalisées	642
Comment fonctionnent les règles de détection personnalisées	643
Sources de données et signaux	643
Modes	644
Trouver une agrégation	645
Champs d'événements expurgés	645
Règles de détection personnalisées disponibles	646
Afficher la logique de détection des règles	647
Fonctions utilisées dans la logique de détection	648
Gestion des règles de détection personnalisées	650
Liste des règles disponibles	650
Affichage de l'état des règles	651
Opérations en vrac	651
Course à sec	652
Direct	653
Désactivation des règles	654
Gestion des règles de détection personnalisées dans les environnements à comptes multiples	654
Configurations d'organisation	655
Exécution des deux modes pour la même règle	656
Exemple : appliquer une règle en mode « run à sec » à tous les comptes membres	657
Appliquer toutes les règles au sein d'une organisation	657
Gestion de plusieurs comptes	659
Relations entre le compte administrateur et le compte membre	660
État de la relation avec les membres	665
Gestion de comptes avec AWS Organizations	666
Considérations et recommandations	667
Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué	669
Désignation d'un compte d'administrateur délégué GuardDuty	671
Configuration des préférences d'activation automatique de l'organisation	672
Ajouter des membres à l'organisation	676
(Facultatif) Activez les plans de protection pour les comptes de membres existants	679
Gérez en permanence vos comptes de membres au sein de GuardDuty	680
Suspension GuardDuty pour compte membre	681
Dissociation (suppression) du compte membre du compte administrateur	683

Supprimer des comptes de membres de GuardDuty l'organisation	685
Modification du compte GuardDuty d'administrateur délégué	686
Gestion des comptes à l'aide des politiques de l'organisation	689
Conditions préalables	689
Comment fonctionnent les politiques de l'organisation	690
Création d'une politique dans la console	693
Examiner l'impact d'une politique avant de l'appliquer	694
Considérations et restrictions	695
Gestion des comptes par invitation	698
Ajouter des comptes sur invitation	699
Consolidation des comptes d'administrateurs au sein d'une seule organisation	704
GuardDuty considérations relatives à l'option Exporter au format CSV dans les comptes	707
Types de résultats	708
Types de résultat EC2	708
Backdoor:EC2/C&CAActivity.B	710
Backdoor:EC2/C&CAActivity.B!DNS	711
Backdoor:EC2/DenialOfService.Dns	712
Backdoor:EC2/DenialOfService.Tcp	713
Backdoor:EC2/DenialOfService.Udp	713
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	714
Backdoor:EC2/DenialOfService.UnusualProtocol	715
Backdoor:EC2/Spambot	715
Behavior:EC2/NetworkPortUnusual	716
Behavior:EC2/TrafficVolumeUnusual	716
CryptoCurrency:EC2/BitcoinTool.B	717
CryptoCurrency:EC2/BitcoinTool.B!DNS	717
DefenseEvasion:EC2/UnusualDNSResolver	718
DefenseEvasion:EC2/UnusualDoHActivity	719
DefenseEvasion:EC2/UnusualDoTActivity	719
Impact:EC2/AbusedDomainRequest.Reputation	720
Impact:EC2/BitcoinDomainRequest.Reputation	720
Impact:EC2/MaliciousDomainRequest.Reputation	721
Impact:EC2/MaliciousDomainRequest.Custom	722
Impact:EC2/PortSweep	722
Impact:EC2/SuspiciousDomainRequest.Reputation	723
Impact:EC2/WinRMBruteForce	723

Recon:EC2/PortProbeEMRUnprotectedPort	724
Recon:EC2/PortProbeUnprotectedPort	725
Recon:EC2/Portscan	726
Trojan:EC2/BlackholeTraffic	727
Trojan:EC2/BlackholeTraffic!DNS	727
Trojan:EC2/DGADomainRequest.B	728
Trojan:EC2/DGADomainRequest.C!DNS	729
Trojan:EC2/DNSDataExfiltration	729
Trojan:EC2/DriveBySourceTraffic!DNS	730
Trojan:EC2/DropPoint	731
Trojan:EC2/DropPoint!DNS	731
Trojan:EC2/PhishingDomainRequest!DNS	732
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	732
UnauthorizedAccess:EC2/MetadataDNSRebind	733
UnauthorizedAccess:EC2/RDPBruteForce	734
UnauthorizedAccess:EC2/SSHBruteForce	735
UnauthorizedAccess:EC2/TorClient	736
UnauthorizedAccess:EC2/TorRelay	736
Types de résultat IAM	737
CredentialAccess:IAMUser/AnomalousBehavior	738
CredentialAccess:IAMUser/CompromisedCredentials	739
DefenseEvasion:IAMUser/AnomalousBehavior	740
DefenseEvasion:IAMUser/BedrockLoggingDisabled	740
Discovery:IAMUser/AnomalousBehavior	741
Exfiltration:IAMUser/AnomalousBehavior	742
Impact:IAMUser/AnomalousBehavior	743
InitialAccess:IAMUser/AnomalousBehavior	743
PenTest:IAMUser/KaliLinux	744
PenTest:IAMUser/ParrotLinux	745
PenTest:IAMUser/PentooLinux	745
Persistence:IAMUser/AnomalousBehavior	746
Policy:IAMUser/RootCredentialUsage	747
Policy:IAMUser/ShortTermRootCredentialUsage	748
PrivilegeEscalation:IAMUser/AnomalousBehavior	748
Recon:IAMUser/MaliciousIPCaller	749
Recon:IAMUser/MaliciousIPCaller.Custom	750

Recon:IAMUser/TorIPCaller	750
Stealth:IAMUser/CloudTrailLoggingDisabled	751
Stealth:IAMUser/PasswordPolicyChange	751
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	752
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	752
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	755
UnauthorizedAccess:IAMUser/MaliciousIPCaller	756
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	757
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	757
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	759
UnauthorizedAccess:IAMUser/TorIPCaller	761
Types de détection de séquences d'attaques	761
AttackSequence:EKS/CompromisedCluster	762
AttackSequence:ECS/CompromisedCluster	763
AttackSequence:EC2/CompromisedInstanceGroup	764
AttackSequence:IAM/CompromisedCredentials	765
AttackSequence:S3/CompromisedData	766
Règles de détection personnalisées : types de recherche	767
Règles de détection personnalisées pour AWS CloudTrail événements de gestion	768
Règles de détection personnalisées pour la surveillance du temps d'exécution	772
Types de détection de la protection S3	778
Discovery:S3/AnomalousBehavior	779
Discovery:S3/MaliciousIPCaller	780
Discovery:S3/MaliciousIPCaller.Custom	781
Discovery:S3/TorIPCaller	781
Exfiltration:S3/AnomalousBehavior	782
Exfiltration:S3/MaliciousIPCaller	783
Impact:S3/AnomalousBehavior.Delete	783
Impact:S3/AnomalousBehavior.Permission	784
Impact:S3/AnomalousBehavior.Write	785
Impact:S3/MaliciousIPCaller	786
PenTest:S3/KaliLinux	786
PenTest:S3/ParrotLinux	787
PenTest:S3/Pentoolinux	787
Policy:S3/AccountBlockPublicAccessDisabled	788
Policy:S3/BucketAnonymousAccessGranted	789

Policy:S3/BucketBlockPublicAccessDisabled	789
Policy:S3/BucketPublicAccessGranted	790
Stealth:S3/ServerAccessLoggingDisabled	791
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	792
UnauthorizedAccess:S3/TorIPCaller	792
Types de recherche de protection EKS	793
CredentialAccess:Kubernetes/MaliciousIPCaller	795
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	795
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	796
CredentialAccess:Kubernetes/TorIPCaller	797
DefenseEvasion:Kubernetes/MaliciousIPCaller	798
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	798
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	799
DefenseEvasion:Kubernetes/TorIPCaller	800
Discovery:Kubernetes/MaliciousIPCaller	800
Discovery:Kubernetes/MaliciousIPCaller.Custom	801
Discovery:Kubernetes/SuccessfulAnonymousAccess	802
Discovery:Kubernetes/TorIPCaller	803
Execution:Kubernetes/ExecInKubeSystemPod	803
Impact:Kubernetes/MaliciousIPCaller	804
Impact:Kubernetes/MaliciousIPCaller.Custom	805
Impact:Kubernetes/SuccessfulAnonymousAccess	805
Impact:Kubernetes/TorIPCaller	806
Persistence:Kubernetes/MaliciousIPCaller	807
Persistence:Kubernetes/MaliciousIPCaller.Custom	807
Persistence:Kubernetes/SuccessfulAnonymousAccess	808
Persistence:Kubernetes/TorIPCaller	809
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	809
Policy:Kubernetes/AnonymousAccessGranted	810
Policy:Kubernetes/ExposedDashboard	811
Policy:Kubernetes/KubeflowDashboardExposed	811
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	812
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	813
Execution:Kubernetes/AnomalousBehavior.ExecInPod	814
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!	
PrivilegedContainer	815

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!	
ContainerWithSensitiveMount	816
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	817
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	818
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	819
Types de recherche liés à la surveillance du temps	820
Recherche des types générés par défaut par Runtime Monitoring	821
Recherche des types nécessitant des règles de détection personnalisées	859
Protection contre les programmes malveillants pour les types de détection EC2	862
Execution:EC2/MaliciousFile	863
Execution:ECS/MaliciousFile	863
Execution:Kubernetes/MaliciousFile	864
Execution:Container/MaliciousFile	864
Execution:EC2/SuspiciousFile	865
Execution:ECS/SuspiciousFile	866
Execution:Kubernetes/SuspiciousFile	866
Execution:Container/SuspiciousFile	867
Protection contre les programmes malveillants pour le type de recherche S3	868
Object:S3/MaliciousFile	868
Protection contre les programmes malveillants pour les types de recherche de Backup	869
Execution:EC2/MaliciousFile!Snapshot	869
Execution:EC2/MaliciousFile!AMI	870
Execution:EC2/MaliciousFile!RecoveryPoint	870
Execution:S3/MaliciousFile!RecoveryPoint	871
Types de résultat de la protection RDS	871
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	872
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	873
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	874
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	875
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	876
Discovery:RDS/MaliciousIPCaller	877
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	877
CredentialAccess:RDS/TorIPCaller.FailedLogin	878
Discovery:RDS/TorIPCaller	879
Exfiltration:RDS/AnomalousBehavior	879
Impact:RDS/AnomalousBehavior.Drop	881

Impact:RDS/AnomalousBehavior.Delete	882
Exfiltration:RDS/MaliciousIPCaller	884
Exfiltration:RDS/TorIPCaller	884
Impact:RDS/MaliciousIPCaller	885
Impact:RDS/TorIPCaller	886
Types de résultat de la protection Lambda	887
Backdoor:Lambda/C&CActivity.B	887
CryptoCurrency:Lambda/BitcoinTool.B	888
Trojan:Lambda/BlackholeTraffic	889
Trojan:Lambda/DropPoint	889
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	890
UnauthorizedAccess:Lambda/TorClient	890
UnauthorizedAccess:Lambda/TorRelay	891
Types de détection de protection contre l'IA	891
Impact:IAMUser/AnomalousModelInvocation	892
Impact:IAMUser/CostHarvesting	894
Impact:IAMUser/PromptInjection.Direct	895
Retrait de types de résultat	897
PrivilegeEscalation:Kubernetes/PrivilegedContainer	899
Persistence:Kubernetes/ContainerWithSensitiveMount	899
Exfiltration:S3/ObjectRead.Unusual	900
Impact:S3/PermissionsModification.Unusual	901
Impact:S3/ObjectDelete.Unusual	901
Discovery:S3/BucketEnumeration.Unusual	902
Persistence:IAMUser/NetworkPermissions	903
Persistence:IAMUser/ResourcePermissions	904
Persistence:IAMUser/UserPermissions	904
PrivilegeEscalation:IAMUser/AdministrativePermissions	905
Recon:IAMUser/NetworkPermissions	906
Recon:IAMUser/ResourcePermissions	907
Recon:IAMUser/UserPermissions	908
ResourceConsumption:IAMUser/ComputeResources	909
Stealth:IAMUser/LoggingConfigurationModified	909
UnauthorizedAccess:IAMUser/ConsoleLogin	910
UnauthorizedAccess:EC2/TorIPCaller	911
Backdoor:EC2/XORDDOS	911

Behavior:IAMUser/InstanceLaunchUnusual	912
CryptoCurrency:EC2/BitcoinTool.A	912
UnauthorizedAccess:IAMUser/UnusualASNCaller	913
GuardDuty recherche de types en fonction des ressources potentiellement affectées	913
GuardDuty types de recherche actifs	914
Comprendre et générer des résultats	940
GuardDuty format de recherche	941
Buts de la menace	942
GuardDuty moteur d'analyse pour la détection des malwares	946
Exemples de résultats	946
Génération d'échantillons de résultats via la GuardDuty console ou l'API	947
Résultats des GuardDuty tests	948
Considérations	949
GuardDuty résultats que le script de testeur peut générer	950
Étape 1 - Prérequis	952
Étape 2 - Déployer AWS les ressources	953
Étape 3 - Exécuter des scripts de test	955
Étape 4 - Nettoyer les ressources AWS de test	957
Dépannage des problèmes courants	958
Page de résultats dans la GuardDuty console	959
Navigation dans la page des résultats	961
Niveaux de gravité des résultats	962
Gravité critique	963
Gravité élevée	963
Gravité moyenne	963
Faible gravité	964
Détails d'un résultat	964
Présentation des résultats	965
Ressource	966
Détails de recherche de la séquence d'attaque	973
Règles de détection personnalisées pour trouver des détails	981
Détails de l'utilisateur de base de données (DB) RDS	983
Surveillance d'exécution : détails des résultats	983
Détails de l'analyse des volumes EBS	986
Protection contre les logiciels malveillants pour la recherche de détails dans EC2	987

Informations sur la recherche effectuée par la protection contre les logiciels malveillants pour S3	988
Action	989
Acteur ou cible	991
Détails de géolocalisation	992
Informations supplémentaires	992
Preuve	993
Comportement anormal	993
GuardDuty recherche d'agrégation	999
Gérer GuardDuty les résultats	1001
GuardDuty Tableau de bord récapitulatif	1002
Présentation de	1003
Résultats	1004
Types de résultat les plus courants	1005
Résultats par gravité	1005
Comptes contenant le plus de résultats	1006
Ressources contenant des résultats	1006
Résultats les moins fréquents	1007
Couverture des plans de protection	1007
Filtrer GuardDuty les résultats	1008
Création et enregistrement d'un ensemble de filtres dans la GuardDuty console	1009
Création et enregistrement d'un ensemble de filtres à l'aide de l' GuardDuty API et de la CLI	1011
métadonnées du cycle de vie	1013
Filtres de propriétés dans GuardDuty	1014
Règles de suppression	1048
Utilisation des règles de suppression avec la détection étendue des menaces	1049
Cas d'utilisation courants des règles de suppression et exemples	1049
Création de règles de suppression	1053
Mettre à jour les règles de suppression	1058
Suppression de règles de suppression	1061
Métriques relatives aux règles de suppression	1062
Listes d'entités et listes d'adresses IP	1064
Comprendre les listes d'entités et les listes d'adresses IP	1064
Considérations importantes relatives aux GuardDuty listes	1065
Formats de liste	1066

Comprendre les statuts des listes	1076
Configuration des prérequis pour les listes d'entités et les listes d'adresses IP	1076
Ajouter et activer une liste d'entités ou une liste d'adresses IP	1079
Mettre à jour une liste d'entités ou une liste d'adresses IP	1085
De-activating liste d'entités ou liste d'adresses IP	1091
Supprimer une liste d'entités ou une liste d'adresses IP	1094
Exportation des résultats générés vers Amazon S3	1097
Considérations	1097
Étape 1 — Autorisations requises pour exporter les résultats	1098
Étape 2 — Associer une politique à votre clé KMS	1099
Étape 3 — Associer une politique au compartiment Amazon S3	1101
Étape 4 - Exportation des résultats vers un compartiment S3 (console)	1105
Étape 5 — Fréquence d'exportation des résultats	1107
Traitement des résultats avec EventBridge	1107
EventBridge fréquence des notifications en GuardDuty	1108
Configurer une rubrique et un point de terminaison Amazon SNS	1109
Utilisation EventBridge avec GuardDuty	1111
Création d'une règle EventBridge	1112
EventBridge règle pour les environnements multi-comptes	1120
Comprendre CloudWatch les journaux et les raisons pour lesquelles des ressources sont ignorées	1121
CloudWatch Journaux d'audit dans GuardDuty Malware Protection pour EC2	1121
GuardDuty Protection contre les programmes malveillants pour la conservation des journaux EC2	1123
Motifs de l'omission des ressources	1124
Signaler un résultat d'analyse de malware EC2 faussement positif	1130
Signaler un résultat d'analyse d'objets S3 faussement positif	1131
Signaler un résultat faussement positif lors de l'analyse des malwares Backup	1132
Correction des résultats	1134
Remédier à une instance Amazon EC2 potentiellement compromise	1134
Remédier à un compartiment S3 potentiellement compromis	1136
Recommandations basées sur les besoins spécifiques d'accès au compartiment S3	1138
Remédier à un objet S3 potentiellement malveillant	1139
Remédier à un instantané EBS potentiellement compromis	1140
Remédier à une AMI EC2 potentiellement compromise	1141
Remédier à un point de restauration EC2 potentiellement compromis	1142

Remédier à un point de restauration S3 potentiellement compromis	1143
Remédier à un cluster ECS potentiellement compromis	1144
Remédier aux failles potentiellement compromises AWS informations d'identification	1145
Remédier à un conteneur autonome potentiellement compromis	1146
Corriger les résultats de la protection EKS	1147
Problèmes de configuration potentiels	1148
Remédier aux utilisateurs de Kubernetes potentiellement compromis	1149
Remédier aux pods Kubernetes potentiellement compromis	1152
Corriger les images de conteneurs potentiellement compromises	1153
Remédier aux nœuds Kubernetes potentiellement compromis	1154
Correction des résultats de la surveillance d'exécution	1155
Correction des images de conteneur compromises	1157
Corriger une base de données potentiellement compromise	1157
Correction d'une base de données potentiellement compromise avec des événements de connexion réussie	1158
Correction d'une base de données potentiellement compromise avec des événements de connexion échouée	1159
Corriger une base de données potentiellement compromise par une activité d'exfiltration anormale	1160
Corriger une base de données potentiellement compromise par une activité destructrice anormale	1162
Correction d'informations d'identification compromises	1163
Retreindre l'accès au réseau	1164
Corriger une fonction Lambda potentiellement compromise	1164
Surveillance de l'utilisation et estimation des coûts	1166
Statistiques CloudWatch d'utilisation d'Amazon	1166
Détails des métriques	1166
Protection contre les programmes malveillants pour S3	1169
Comprendre GuardDuty l'utilisation	1170
GuardDuty Traitement des événements	1170
GuardDuty Frais de traitement des journaux de flux VPC pour les instances surveillées par GuardDuty Runtime Monitoring	1171
Estimation des GuardDuty coûts	1171
Utilisation AWS Calculateur de prix	1172
Clients de Security Hub	1172
Noms des fonctionnalités pour les plans de protection dans l'API	1174

Passer des sources de données aux fonctionnalités	1174
GuardDuty Modifications de l'API	1175
Caractéristiques comparées aux sources de données	1175
Comprendre le fonctionnement des API dotées de fonctionnalités	1176
Intégration des modifications apportées aux fonctionnalités dans les API	1176
Fonctionnalité mappée GuardDuty	1177
Sécurité	1180
Protection des données	1181
Chiffrement au repos	1182
Chiffrement en transit	1182
Refus d'utiliser vos données pour améliorer le service	1182
Se connecter avec CloudTrail	1184
GuardDuty informations dans CloudTrail	1185
GuardDuty événements du plan de contrôle dans CloudTrail	1186
GuardDuty événements de données dans CloudTrail	1186
Exemple : entrées de fichier GuardDuty journal	1187
Gestion de l'identité et des accès	1190
Public ciblé	1190
Authentification par des identités	1191
Gestion de l'accès à l'aide de politiques	1192
Comment Amazon GuardDuty travaille avec IAM	1194
Identity-based exemples de politiques	1200
Utilisation des rôles liés à un service	1210
AWS politiques gérées	1221
Résolution des problèmes	1238
Validation de conformité	1241
Résilience	1241
Sécurité de l'infrastructure	1241
Points de terminaison de VPC (AWS PrivateLink)	1242
Considérations relatives aux points de GuardDuty terminaison VPC	1242
Création d'un point de terminaison VPC d'interface pour GuardDuty	1243
Création d'une politique de point de terminaison VPC pour GuardDuty	1243
Sous-réseaux partagés	1244
Intégration aux services AWS de sécurité	1245
Intégration GuardDuty avec AWS Security Hub CSPM	1245
Intégration GuardDuty à Amazon Detective	1245

AWS Security Hub CSPM intégration	1245
Comment Amazon GuardDuty envoie ses résultats à AWS Security Hub CSPM	1246
Afficher GuardDuty les résultats dans AWS Security Hub CSPM	1247
Activation et configuration de l'intégration	1268
Utilisation GuardDuty des contrôles dans Security Hub CSPM	1268
Arrêt de la publication des résultats sur Security Hub CSPM	1268
Intégration avec Amazon Detective	1268
Activation de l'intégration	1269
Passer à Amazon Detective à partir d'une découverte GuardDuty	1269
Utilisation de l'intégration avec un environnement GuardDuty multi-comptes	1270
Suspension ou désactivation	1271
GuardDuty annonces	1273
Format du message Amazon SNS	1279
GuardDuty quotas	1285
Support pour les instances gérées	1292
Résolution des problèmes	1293
Exportation des résultats vers Amazon S3 : erreur d'accès	1293
Protection contre les programmes malveillants pour les problèmes liés à EC2	1294
Manquant (obligatoire) AWS Organizations autorisation de gestion lors de l'activation de l'analyse des GuardDuty-initiated programmes malveillants	1294
Je lance une analyse des On-demand logiciels malveillants, mais cela entraîne une erreur d'autorisation requise manquante.	1294
Je reçois un message d'GetRoleerreur iam : lors de l'utilisation de Malware Protection for EC2.	1295
Je suis un compte GuardDuty administrateur qui doit activer le scan des GuardDuty-initiated logiciels malveillants mais qui n'utilise pas AWS politique gérée : AmazonGuardDutyFullAccess à gérer GuardDuty.	1295
Problèmes de surveillance du temps d'exécution	1295
Problèmes de couverture du temps d'exécution	1295
Résolution d'une erreur de mémoire insuffisante	1296
Mon AWS Step Functions le flux de travail échoue de façon inattendue	1297
Autres problèmes de résolution des problèmes	1297
Régions et points de terminaison	1298
Region-specific disponibilité des fonctionnalités	1298
Actions et paramètres hérités	1301
Historique de la documentation	1303

Mises à jour antérieures	1422
.....	mcdxxiii

Qu'est-ce qu'Amazon GuardDuty ?

Amazon GuardDuty est un service de détection des menaces qui surveille, analyse et traite en permanence les sources de AWS données et les journaux de votre AWS environnement. GuardDuty utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, des hachages de fichiers et des modèles d'apprentissage automatique (ML) pour identifier les activités suspectes et potentiellement malveillantes dans votre AWS environnement. La liste suivante fournit une vue d'ensemble des scénarios de menaces potentiels qui GuardDuty peuvent vous aider à les détecter :

- Informations d'identification compromises et exfiltrées. AWS
- Exfiltration et destruction de données susceptibles de provoquer un ransomware. Modèles inhabituels d'événements de connexion dans les versions de moteur prises en charge des bases de données Amazon Aurora et Amazon RDS, qui indiquent un comportement anormal.
- Activité de cryptomining non autorisée dans vos instances Amazon Elastic Compute Cloud (Amazon EC2) et dans vos charges de travail de conteneurs.
- Présence de logiciels malveillants dans vos instances Amazon EC2 et vos charges de travail de conteneur, et de fichiers récemment téléchargés dans vos compartiments Amazon Simple Storage Service (Amazon S3).
- Événements au niveau du système d'exploitation, du réseau et des fichiers indiquant un comportement non autorisé sur vos clusters Amazon Elastic Kubernetes Service (Amazon EKS), sur vos tâches Amazon Elastic Container Service (Amazon ECS), sur vos instances Amazon AWS Fargate EC2 et sur vos charges de travail de conteneur.

La vidéo suivante donne un aperçu de la manière dont vous pouvez GuardDuty détecter les menaces dans votre AWS environnement.

[Qu'est-ce qu'Amazon GuardDuty](#)

Table des matières

- [Caractéristiques de GuardDuty](#)
- [Conformité PCI DSS](#)
- [Tarification en GuardDuty](#)
- [Accès GuardDuty](#)

Caractéristiques de GuardDuty

Voici quelques-uns des principaux moyens par lesquels Amazon GuardDuty peut vous aider à surveiller, détecter et gérer les menaces potentielles dans votre AWS environnement.

Surveillance en permanence des sources de données et des journaux d'événements spécifiques

- **Détection des menaces fondamentales** : lorsque vous activez un Compte AWS, commence GuardDuty automatiquement GuardDuty à ingérer les sources de données de base associées à ce compte. Ces sources de données incluent les événements AWS CloudTrail de gestion, les journaux de flux VPC (provenant d'instances Amazon EC2) et les journaux DNS. Vous

n'avez rien d'autre à activer pour commencer GuardDuty à analyser et à traiter ces sources de données afin de générer les résultats de sécurité associés. Pour plus d'informations, consultez [GuardDuty sources de données de base](#).

- **Détection étendue des menaces** — Cette fonctionnalité détecte les attaques en plusieurs étapes qui couvrent les sources de données fondamentales, plusieurs types de AWS ressources et le temps, au sein d'un. Compte AWS Il se peut que plusieurs événements se produisent dans votre compte qui, pris isolément, ne constituent pas une menace claire. Toutefois, lorsque ces événements sont observés dans une séquence indiquant une activité suspecte, il s'agit d'une séquence d'attaque. GuardDuty vous avertit en générant le type de recherche de séquence d'attaque associé pour fournir des détails sur la séquence d'attaque observée.

Sans frais supplémentaires, la détection étendue des menaces est automatiquement activée pour chacun d'entre eux Compte AWS lorsqu'ils sont activés GuardDuty. Cette fonctionnalité ne vous oblige pas à activer un plan de protection axé sur les cas d'utilisation. Toutefois, pour renforcer la sécurité de vos ressources Amazon S3, il est recommandé d'activer S3 Protection dans votre compte. Cela aidera Extended Threat Detection à identifier les attaques en plusieurs étapes susceptibles d'avoir un impact sur vos ressources Amazon S3.

Pour plus d'informations sur le fonctionnement de cette fonctionnalité et les scénarios de menace qu'elle couvre, consultez [GuardDuty Détection étendue des menaces](#).

- **Investigation (aperçu)** — GuardDuty Investigation fournit une analyse de AI-powered sécurité de vos GuardDuty résultats. Vous pouvez créer des enquêtes pour analyser des résultats spécifiques, des comptes ou l'ensemble de votre organisation, et recevoir des résumés d'enquêtes structurés avec une évaluation des risques, un score de confiance, une classification MITRE ATT&CK® et les prochaines étapes réalisables. Pour plus d'informations, consultez [GuardDuty Enquête \(aperçu\)](#).
- **Règles de détection personnalisées** — Les règles de détection personnalisées sont une bibliothèque organisée de règles de détection sur Amazon GuardDuty qui sont alignées sur les techniques des auteurs de menaces. Chaque règle détecte une technique spécifique en évaluant les champs des événements de AWS CloudTrail gestion ou des événements de surveillance du temps d'exécution fournis par l'agent de GuardDuty sécurité. Vous pouvez parcourir, activer et gérer les règles depuis la GuardDuty console ou via l' API GuardDuty. Pour plus d'informations, consultez [Règles de détection personnalisées dans GuardDuty](#).
- **Use-case plans de GuardDuty protection ciblés** : pour améliorer la visibilité de la détection des menaces sur la sécurité de votre AWS environnement, GuardDuty propose des plans

de protection dédiés que vous pouvez choisir d'activer. Les plans de protection vous aident à surveiller les journaux et les événements provenant d'autres AWS services. Ces sources incluent les journaux d'audit EKS, l'activité de connexion RDS, les événements liés aux données Amazon S3 CloudTrail, les volumes EBS, la surveillance du temps d'exécution sur Amazon EKS, Amazon EC2 et Amazon ECS-Fargate, les journaux d'activité du réseau Lambda et les événements de AWS CloudTrail données provenant d'Amazon Bedrock AgentCore, Amazon Bedrock et Amazon AI for AI Protection. SageMaker GuardDuty consolide ces sources de journaux et d'événements sous le terme « [Fonctionnalités](#) ». Vous pouvez activer à tout moment un ou plusieurs plans de protection dédiés dans un Région AWS programme pris en charge. GuardDuty commencera à surveiller, traiter et analyser les activités en fonction du plan de protection que vous activez. Pour plus d'informations sur chaque plan de protection et son fonctionnement, consultez le document du plan de protection correspondant.

Lorsque vous l'activez GuardDuty pour la première fois, tous les plans de protection GuardDuty sont automatiquement activés, à l'exception de la surveillance du temps d'exécution pour votre compte, et ils sont inclus dans l'essai gratuit de 30 jours. Vous pouvez désactiver n'importe quel plan de protection à tout moment. Si vous êtes déjà GuardDuty client, un plan de protection lancé une fois que vous l'avez activé n' GuardDuty est pas activé automatiquement, et vous pouvez choisir de l'activer. Pour plus d'informations sur les plans de protection activés par défaut, consultez [Utilisation de l' GuardDuty essai gratuit de 30 jours](#).

Plan de protection	Description
Protection de l'IA	Détecte les menaces qui pèsent sur vos charges de travail basées sur l'IA qui utilisent Amazon Bedrock, Amazon Bedrock AgentCore et Amazon SageMaker AI, telles que les invocations de modèles anormales et les attaques de collecte des coûts.
Protection S3	Identifie les risques de sécurité potentiels tels que l'exfiltration de données et les tentatives de destruction dans vos compartiments Amazon S3.
Protection EKS	EKS Audit Log Monitoring analyse les journaux d'audit Kubernetes de vos clusters Amazon EKS pour détecter les activités potentiellement suspectes et malveillantes.

Plan de protection	Description
Surveillance d'exécution	Surveille et analyse les événements au niveau du système d'exploitation sur votre Amazon EKS, Amazon EC2 et Amazon ECS (AWS Fargate y compris), afin de détecter les menaces d'exécution potentielles.
Protection contre les logiciels malveillants pour EC2	Détecte la présence potentielle de logiciels malveillants en analysant les volumes Amazon EBS associés à vos instances Amazon EC2. Il existe une option permettant d'utiliser cette fonctionnalité à la demande.
Protection contre les logiciels malveillants pour S3	Détecte la présence potentielle de logiciels malveillants dans les objets récemment chargés dans vos compartiments Amazon S3. Il existe une option permettant d'utiliser cette fonctionnalité à la demande.
Protection contre les logiciels malveillants pour AWS Backup	Détecte la présence potentielle de logiciels malveillants en analysant les ressources de sauvegarde, notamment les instantanés EBS, les AMI EC2 et les points de restauration des AWS sauvegardes. Il existe une option permettant d'utiliser cette fonctionnalité à la demande.
Protection RDS	Analyse et profile votre activité de connexion RDS pour détecter les menaces d'accès potentielles aux bases de données Amazon Aurora et Amazon RDS prises en charge.
Protection Lambda	Surveille les journaux d'activité du réseau Lambda, en commençant par les journaux de flux VPC, afin de détecter les menaces qui pèsent sur vos fonctions. AWS Lambda Le minage de cryptomonnaies et la communication avec des serveurs malveillants sont des exemples de ces menaces potentielles.

- ❗ Activez la protection contre les programmes malveillants pour S3 de manière indépendante

GuardDuty offre la possibilité d'utiliser Malware Protection for S3 de manière indépendante, sans activer le GuardDuty service Amazon. Pour plus d'informations sur la mise en route uniquement avec Malware Protection pour S3, consultez [GuardDuty Protection contre les logiciels malveillants pour S3](#). Pour utiliser tous les autres plans de protection, vous devez activer le GuardDuty service.

Gestion d'un environnement à comptes multiples

Vous pouvez gérer un AWS environnement à comptes multiples en utilisant une méthode d'invitation AWS Organizations (recommandée) ou une ancienne méthode d'invitation. Pour plus d'informations, consultez [Gestion de plusieurs comptes](#).

Génère des résultats de sécurité pour les menaces détectées

Lorsqu'il GuardDuty détecte des menaces de sécurité potentielles associées à vos AWS ressources, il commence à générer des résultats de sécurité fournissant des informations sur la ressource potentiellement compromise. Une fois que vous l'avez activé GuardDuty dans votre compte, générez [Exemples de résultats](#) pour afficher les informations associées [Détails d'un résultat](#). Pour une liste complète des résultats de sécurité, voir [GuardDuty types de recherche](#).

Avec GuardDuty, vous pouvez également utiliser un script de test qui génère des résultats GuardDuty de sécurité spécifiques pour comprendre comment examiner les GuardDuty résultats et y répondre. Pour plus d'informations, consultez [GuardDuty Résultats des tests dans des comptes dédiés](#).

Évaluation et gestion des résultats de sécurité

GuardDuty consolide vos résultats de sécurité sur l'ensemble des comptes et affiche les résultats dans le tableau de bord récapitulatif de la GuardDuty console. Vous pouvez également récupérer les résultats via l' AWS Security Hub CSPM API ou le AWS SDK. AWS Command Line Interface Grâce à une vision globale de votre état de sécurité actuel, vous pouvez identifier les tendances et les problèmes potentiels, et prendre les mesures correctives nécessaires. Pour plus d'informations, consultez [Gérer GuardDuty les résultats](#).

Intégrez les services AWS de sécurité connexes

Pour vous aider à analyser et à étudier les tendances en matière de sécurité dans votre AWS environnement, pensez à utiliser les services AWS liés à la sécurité suivants en combinaison avec GuardDuty

- **AWS Security Hub CSPM**— Ce service vous donne une vue complète de l'état de sécurité de vos AWS ressources et vous aide à vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Pour ce faire, il utilise, agrège, organise et hiérarchise les résultats de sécurité provenant de multiples AWS services (y compris Amazon Macie) et de produits du réseau de partenaires (APN) AWS pris en charge. Security Hub CSPM vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires dans votre AWS environnement.

Pour plus d'informations sur l'utilisation GuardDuty conjointe de Security Hub CSPM, consultez [Intégration GuardDuty avec AWS Security Hub CSPM](#) Pour en savoir plus sur Security Hub CSPM, consultez le guide de l'[AWS Security Hub utilisateur](#).

- **Amazon Detective** : ce service vous permet d'analyser, d'enquêter et d'identifier rapidement la cause première des problèmes de sécurité ou des activités suspectes. Detective collecte automatiquement les données du journal à partir de vos AWS ressources. Detective utilise ensuite le machine learning, l'analyse statistique et la théorie des graphes pour générer des visualisations qui vous aideront à mener des investigations de sécurité plus rapides et plus efficaces. Les agrégations de données prédéfinies, les résumés et le contexte du Detective vous aident à analyser et à déterminer la nature et l'étendue des problèmes de sécurité potentiels.

Pour plus d'informations sur l'utilisation conjointe de Detective GuardDuty et de Detective, consultez [Intégration GuardDuty à Amazon Detective](#). Pour en savoir plus sur Detective, consultez le [guide de l'utilisateur d'Amazon Detective](#).

- **Amazon EventBridge** — Ce service vous permet de recevoir des notifications et de répondre aux GuardDuty problèmes de sécurité en temps quasi réel. GuardDuty crée un événement en cas de modification des résultats. Vous pouvez choisir la fréquence à laquelle vous souhaitez recevoir les notifications EventBridge. Pour plus d'informations, consultez [What is Amazon EventBridge](#) dans le guide de EventBridge l'utilisateur Amazon.

Conformité PCI DSS

GuardDuty prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et sa conformité à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) a été validée. Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section [PCI DSS niveau 1](#).

Pour plus d'informations, consultez la section [Nouveau test tiers comparant Amazon GuardDuty aux systèmes de détection d'intrusion sur le réseau](#) dans le blog sur la AWS sécurité.

Tarification en GuardDuty

Cette section se concentre sur le Niveau gratuit d'AWS modèle GuardDuty utilisé pour les différents plans de protection et sur la manière dont vous pouvez consulter les coûts d'utilisation estimés et réels. Si vous recherchez le détail des tarifs associés à tous les plans de protection dans les régions prises en charge, consultez [GuardDutyles tarifs](#).

Niveau gratuit d'AWS

Niveau gratuit d'AWS vous permet d'explorer et d'essayer Services AWS gratuitement jusqu'à des limites spécifiées pour chaque service. Il existe trois catégories : 12 mois gratuits, toujours gratuits et essais gratuits de courte durée. Amazon GuardDuty appartient à la catégorie des essais gratuits de courte durée et propose un essai gratuit de 30 jours. Lorsque vous continuez à utiliser ce GuardDuty service après la fin de cet essai gratuit, vous commencez à encourir des frais en fonction de la façon dont vous utilisez ce service.

¹ Exception à l' GuardDuty essai gratuit de 30 jours

On-demand l'analyse des programmes malveillants (sous Malware Protection pour EC2) et la protection contre les logiciels malveillants pour S3 ne sont pas incluses dans la catégorie des essais gratuits de courte durée de GuardDuty 30 jours. Malware Protection for S3 inclut un niveau gratuit, tandis que l'analyse des On-demand programmes malveillants suit un modèle de coût basé sur le paiement à l'utilisation. Il n'existe pas d'essai gratuit de 30 jours ni de modèle de coût gratuit avec analyse des On-demand logiciels malveillants.

Utilisation de l' GuardDuty essai gratuit de 30 jours

Lorsque vous l'utilisez GuardDuty pour la première fois depuis une Région AWS, vous Compte AWS êtes automatiquement inscrit à un essai gratuit de 30 jours dans cette région. Certains plans de protection seront également activés automatiquement et sont inclus dans l'essai gratuit de 30 jours. Comme il GuardDuty s'agit d'un service régional, lorsque vous l'activez pour la première fois dans une autre région, votre compte bénéficie d'un essai gratuit de 30 jours GuardDuty dans cette région. Lorsque vous travaillez avec plusieurs comptes au sein d'une GuardDuty organisation, chaque compte bénéficie de son propre essai gratuit de 30 jours.

Utilisez le tableau suivant pour connaître les plans de protection activés par défaut et leur disponibilité en version d'essai gratuite. GuardDuty

Plan de protection	Activé par défaut avec GuardDuty	Disponibilité d'essai gratuite séparée ²	
Protection EKS	Oui	Oui	
Protection S3	Oui	Oui	
Surveillance d'exécution	Non	Oui	
Protection contre les logiciels malveillants pour EC2 – GuardDuty-initiated analyse des logiciels malveillants	Oui	Oui	
Protection contre les logiciels malveillants pour EC2 – On-demand analyse des logiciels malveillants dans GuardDuty	Non	Non ¹	

Plan de protection	Activé par défaut avec GuardDuty	Disponibilité d'essai gratuite séparée ²	
GuardDuty Protection contre les logiciels malveillants pour S3	Non	Non ¹	
Protection RDS	Oui	Oui	
Protection Lambda	Oui	Oui	
Protection contre les logiciels malveillants pour AWS Backup	Non	Non	

² Lorsque vous activez GuardDuty pour la première fois, les plans de protection (à l'exception de la surveillance du temps d'exécution) sont automatiquement activés et inclus dans l'essai gratuit initial de 30 jours. Lorsqu'un compte GuardDuty existant active un nouveau plan de protection après l'expiration de son essai GuardDuty gratuit initial, ce plan de protection est assorti de son propre essai gratuit de 30 jours. Pour plus d'informations sur les essais gratuits des plans de protection, consultez le document associé à chaque plan de protection.

Afficher le coût d'utilisation estimé pendant l'essai gratuit — Au cours de l'essai gratuit de 30 jours GuardDuty et éventuellement d'un plan de protection, GuardDuty fournit une estimation du coût d'utilisation de votre compte. Si vous êtes un compte GuardDuty administrateur délégué, vous pouvez consulter le coût d'utilisation total estimé et la répartition au niveau du compte pour tous les comptes membres qui ont été activés. Pour plus d'informations, consultez [Surveillance de GuardDuty l'utilisation et estimation des coûts](#).

Coût d'utilisation après la fin de l'essai gratuit — Lorsque vous continuez à utiliser l' GuardDuty un de ses plans de protection après la fin de l'essai gratuit, vous commencez à encourir des frais d'utilisation associés. Pour consulter votre facture, accédez à Cost Explorer dans la <https://console.aws.amazon.com/costmanagement/console>. Pour plus d'informations sur la facturation du AWS compte, consultez le [guide de AWS Billing l'utilisateur](#).

Utilisation de la protection contre les programmes malveillants pour S3 avec le niveau gratuit

Malware Protection for S3 inclut un niveau gratuit associé à votre Comptes AWS. Pour plus d'informations, consultez [Tarification et coût d'utilisation de Malware Protection for S3](#).

Accès GuardDuty

Amazon GuardDuty est disponible dans la plupart des pays Régions AWS. Pour une liste des régions où cette GuardDuty option est actuellement disponible, consultez [Régions et points de terminaison](#).

Vous pouvez l'utiliser GuardDuty de l'une des manières suivantes :

GuardDuty console

<https://console.aws.amazon.com/guardduty/>

La console est une interface basée sur un navigateur qui permet d'accéder à GuardDuty et de l'utiliser. La GuardDuty console permet d'accéder à votre GuardDuty compte, à vos données et à vos ressources.

AWS Command Line Interface

Avec AWS Command Line Interface (AWS CLI), vous pouvez émettre des commandes sur la ligne de commande de votre système pour effectuer des GuardDuty tâches et AWS des tâches. Les AWS CLI commandes sont utiles si vous souhaitez créer des scripts qui exécutent des tâches.

Pour plus d'informations sur l'installation et l'utilisation AWS CLI, consultez le [Guide de AWS Command Line Interface l'utilisateur](#). Pour consulter les AWS CLI commandes disponibles pour GuardDuty, consultez la section [Référence des AWS CLI commandes](#).

GuardDuty API HTTPS

Vous pouvez y accéder GuardDuty et par AWS programmation en utilisant l'API GuardDuty HTTPS, qui vous permet d'envoyer des requêtes HTTPS directement au service. Pour plus d'informations, consultez le [Amazon GuardDuty API Reference](#).

AWS SDK

AWS fournit des kits de développement logiciel (SDK) composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Python, Ruby, .NET,

iOS, Android, etc.). Ils facilitent la création par programmation d'un accès à GuardDuty. Pour en savoir plus sur les kits de développement logiciel AWS , y compris les procédures pour les télécharger et les installer, consultez [Outils pour Amazon Web Services](#).

Concepts et termes clés sur Amazon GuardDuty

Lorsque vous débutez avec Amazon GuardDuty, vous pouvez tirer parti de l'apprentissage de ses concepts et des termes clés associés.

Compte

Un compte Amazon Web Services (AWS) standard contenant vos AWS ressources. Vous pouvez vous connecter AWS à votre compte et l'activer GuardDuty.

Vous pouvez également inviter d'autres comptes à activer votre AWS compte GuardDuty et à s'y associer dans GuardDuty. Si vos invitations sont acceptées, votre compte est désigné comme GuardDuty compte administrateur et les comptes ajoutés deviennent vos comptes de membre. Vous pouvez ensuite consulter et gérer les GuardDuty résultats de ces comptes en leur nom.

Les utilisateurs du compte administrateur peuvent configurer GuardDuty , consulter et gérer les GuardDuty résultats pour leur propre compte et pour tous leurs comptes membres. Pour plus d'informations sur le nombre de comptes de membres que votre compte administrateur peut gérer, consultez [GuardDuty quotas](#).

Les utilisateurs des comptes membres peuvent configurer GuardDuty , consulter et gérer les GuardDuty résultats de leur compte (via la console GuardDuty de gestion ou l' GuardDuty API). Les utilisateurs de comptes membres ne peuvent pas afficher ou gérer des résultats dans les comptes d'autres membres.

Un compte AWS ne peut pas être un compte GuardDuty administrateur et un compte membre en même temps. Un compte AWS peut accepter qu'une seule invitation d'adhésion. L'acceptation d'une invitation d'adhésion est facultative.

Pour de plus amples informations, veuillez consulter [Gérer plusieurs comptes sur Amazon GuardDuty](#).

Séquence d'attaque

Une séquence d'attaque est une corrélation entre plusieurs événements qui, tels qu'observés par GuardDuty, se sont produits dans une séquence spécifique correspondant au schéma d'une activité suspecte. GuardDuty utilise sa [Détection étendue des menaces](#) capacité pour détecter ces attaques en plusieurs étapes qui concernent les sources de données, les AWS ressources et le calendrier fondamentaux de votre compte.

La liste suivante explique brièvement les termes clés associés aux séquences d'attaque :

- **Indicateurs** — Fournit des informations expliquant pourquoi une séquence d'événements correspond à une activité suspecte potentielle.
- **Signaux** — Un signal est une activité d'API GuardDuty observée ou une GuardDuty découverte déjà détectée dans votre compte. En corrélant les événements observés dans une séquence spécifique dans votre compte, vous GuardDuty identifiez une séquence d'attaque.

Certains événements de votre compte ne sont pas révélateurs d'une menace potentielle. GuardDuty les considère comme des signaux faibles. Cependant, lorsque des signaux faibles et des GuardDuty résultats sont observés dans une séquence spécifique qui, lorsqu'ils sont corrélés, correspondent à une activité potentiellement suspecte, GuardDuty génère une détection de séquence d'attaque.

- **Points de terminaison** : informations sur les points de terminaison du réseau potentiellement utilisés par un acteur malveillant dans une séquence d'attaque.

Détecteur

Amazon GuardDuty est un service régional. Lorsque vous l'activez GuardDuty dans un domaine spécifique Région AWS, vous Compte AWS êtes associé à un identifiant de détecteur. Cet identifiant alphanumérique à 32 caractères est unique à votre compte dans cette région. Par exemple, lorsque vous activez GuardDuty le même compte dans une région différente, votre compte sera associé à un identifiant de détecteur différent. Le format d'un ID de détecteur est 12abc34d567e8fa901bc2d34e56789f0.

Tous les GuardDuty résultats, comptes et actions relatifs à la gestion des résultats et au GuardDuty service utilisent un identifiant de détecteur pour exécuter une opération d'API.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

Note

Dans des environnements à plusieurs comptes, tous les résultats destinés aux comptes membres sont associés au détecteur du compte administrateur.

Certaines GuardDuty fonctionnalités sont configurées via le détecteur, telles que la configuration de la fréquence de notification des CloudWatch événements et l'activation ou la désactivation de plans de protection facultatifs GuardDuty à traiter.

Utilisation de la protection contre les programmes malveillants pour S3 dans GuardDuty

Lorsque vous activez la protection contre les programmes malveillants pour S3 dans un compte où cette option GuardDuty est activée, les actions de protection contre les programmes malveillants pour S3 telles que l'activation, la modification et la désactivation d'une ressource protégée ne sont pas associées à l'ID du détecteur.

Lorsque vous n'activez pas GuardDuty et ne choisissez pas l'option de détection des menaces Malware Protection for S3, aucun identifiant de détecteur n'est créé pour votre compte.

Sources de données de base

Origine ou emplacement d'un ensemble de données. Pour détecter une activité non autorisée ou inattendue dans votre AWS environnement. GuardDuty analyse et traite les données provenant des journaux d' AWS CloudTrail événements, AWS CloudTrail des événements de gestion, AWS CloudTrail des événements de données pour S3, des journaux de flux VPC, des journaux DNS, voir. [GuardDuty sources de données de base](#)

Fonctionnalité

Un objet fonctionnel configuré pour votre plan de GuardDuty protection permet de détecter une activité non autorisée ou inattendue dans votre AWS environnement. Chaque plan de GuardDuty protection configure l'objet fonctionnel correspondant pour analyser et traiter les données. Parmi les objets de fonctionnalité, citons les journaux d'audit EKS, la surveillance de l'activité de connexion RDS, les journaux d'activité du réseau Lambda et les volumes EBS. Pour de plus amples informations, veuillez consulter [Noms des fonctionnalités pour les plans de protection dans GuardDuty l'API](#).

Résultat

Un problème potentiel de sécurité a été détecté par GuardDuty. Pour de plus amples informations, veuillez consulter [Comprendre et générer des GuardDuty résultats sur Amazon](#).

Les résultats sont affichés dans la GuardDuty console et contiennent une description détaillée du problème de sécurité. Vous pouvez également récupérer les résultats que vous avez générés en appelant les opérations [GetFindingset](#) [ListFindings](#)API.

Vous pouvez également consulter vos GuardDuty résultats par le biais CloudWatch des événements Amazon. GuardDuty envoie les résultats à Amazon CloudWatch via le protocole HTTPS. Pour de plus amples informations, veuillez consulter [Traitement des GuardDuty résultats avec Amazon EventBridge](#).

Rôle IAM

Il s'agit du rôle IAM disposant des autorisations requises pour scanner l'objet S3. Lorsque le balisage des objets numérisés est activé, les PassRole autorisations IAM permettent d'ajouter des balises à l'objet numérisé.

Ressource du plan de protection contre les logiciels

Après avoir activé la protection contre les programmes malveillants pour S3 pour un compartiment, il GuardDuty crée une ressource de plan de protection contre les programmes malveillants. Cette ressource est associée à l'ID du plan de protection contre les malwares, un identifiant unique pour votre compartiment protégé. Utilisez la ressource du plan Malware Protection pour effectuer des opérations d'API sur une ressource protégée.

Bucket protégé (ressource protégée)

Un compartiment Amazon S3 est considéré comme protégé lorsque vous activez Malware Protection for S3 pour ce compartiment et que son statut de protection passe à Active.

GuardDuty prend uniquement en charge un compartiment S3 en tant que ressource protégée.

État de protection

État associé à la ressource de votre plan de protection contre les programmes malveillants. Une fois que vous avez activé Malware Protection for S3 pour votre compartiment, cet état indique si votre compartiment est correctement configuré ou non.

Préfixe d'objet S3

Dans un bucket Amazon Simple Storage Service (Amazon S3), vous pouvez utiliser des préfixes pour organiser votre stockage. Un préfixe est un regroupement logique des objets d'un compartiment S3. Pour plus d'informations, consultez la section [Organisation et mise en liste des objets](#) dans le guide de l'utilisateur Amazon S3.

Options de numérisation

Lorsque la protection contre les GuardDuty programmes malveillants pour EC2 est activée, elle vous permet de spécifier les instances Amazon EC2 et les volumes Amazon Elastic Block Store (EBS) à scanner ou à ignorer. Cette fonctionnalité vous permet d'ajouter les balises existantes associées à vos instances EC2 et à votre volume EBS à une liste de balises d'inclusion ou d'exclusion. Les ressources associées aux balises que vous ajoutez à une liste de balises d'inclusion sont analysées pour détecter les logiciels malveillants, et celles ajoutées à une liste de balises d'exclusion ne sont pas analysées. Pour de plus amples informations, veuillez consulter [Options d'analyse avec balises définies par l'utilisateur](#).

Conservation des instantanés

Lorsque GuardDuty Malware Protection for EC2 est activée, elle offre la possibilité de conserver les instantanés de vos volumes EBS dans votre compte. AWS GuardDuty génère les volumes EBS répliqués en fonction des instantanés de vos volumes EBS. Vous ne pouvez conserver les instantanés de vos volumes EBS que si le scan Malware Protection for EC2 détecte des malwares dans les répliques des volumes EBS. Si aucun logiciel malveillant n'est détecté dans les volumes EBS répliqués, supprime GuardDuty automatiquement les instantanés de vos volumes EBS, quel que soit le paramètre de conservation des instantanés. Pour de plus amples informations, veuillez consulter [Conservation des instantanés](#).

Règle de suppression

Les règles de suppression vous permettent de créer des combinaisons d'attributs très spécifiques pour supprimer des résultats. Par exemple, vous pouvez définir une règle via le GuardDuty filtre pour archiver automatiquement Recon : EC2/Portscan uniquement les instances d'un VPC spécifique, d'une AMI spécifique ou d'une balise EC2 spécifique. Cette règle entraînerait l'archivage automatique des résultats d'analyse de port depuis les instances qui répondent aux critères. Cependant, il permet toujours d'émettre des alertes s'il GuardDuty détecte des instances menant d'autres activités malveillantes, telles que le minage de cryptomonnaies.

Les règles de suppression définies dans le compte GuardDuty administrateur s'appliquent aux comptes des GuardDuty membres. GuardDuty les comptes membres ne peuvent pas modifier les règles de suppression.

Avec les règles de suppression, génère GuardDuty toujours tous les résultats. Les règles de suppression permettent de supprimer des résultats tout en conservant un historique immuable et complet de toute l'activité.

En général, les règles de suppression sont utilisées pour masquer les résultats que vous avez déterminés comme faux positifs pour votre environnement et limitent les perturbations provenant des résultats de faible valeur afin de vous permettre de vous concentrer sur les menaces plus importantes. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

Liste d'adresses IP approuvées

Une liste d'adresses IP fiables pour une communication hautement sécurisée avec votre AWS environnement. GuardDuty ne génère pas de résultats basés sur des listes d'adresses IP fiables. Pour de plus amples informations, veuillez consulter [Personnalisation de la détection des menaces à l'aide de listes d'entités et de listes d'adresses IP](#).

Liste d'adresses IP de menaces

Liste d'adresses IP malveillantes. En plus de générer des résultats en raison d'une activité potentiellement suspecte, il génère GuardDuty également des résultats basés sur ces listes de menaces. Pour de plus amples informations, veuillez consulter [Personnalisation de la détection des menaces à l'aide de listes d'entités et de listes d'adresses IP](#).

Commencer avec GuardDuty

Ce didacticiel fournit une introduction pratique à GuardDuty. Les exigences minimales pour l'activation GuardDuty en tant que compte autonome ou en tant qu'administrateur AWS Organizations sont décrites à l'étape 1. Les étapes 2 à 5 couvrent l'utilisation des fonctionnalités supplémentaires recommandées par GuardDuty pour tirer le meilleur parti de vos résultats.

Rubriques

- [Avant de commencer](#)
- [Étape 1 : activer Amazon GuardDuty](#)
- [Étape 2 : générer des exemples de résultats et explorer les opérations de base](#)
- [Étape 3 : configurer l'exportation GuardDuty des résultats vers un compartiment Amazon S3](#)
- [Étape 4 : configurer les alertes de GuardDuty recherche via SNS](#)
- [Étapes suivantes](#)

Avant de commencer

GuardDuty est un service de détection des menaces qui surveille [Source de données de base](#) notamment les événements AWS CloudTrail de gestion, les journaux de flux Amazon VPC et les journaux de requêtes Amazon Route 53 Resolver DNS. GuardDuty analyse également les fonctionnalités associées à ses types de protection uniquement si vous les activez séparément. Les [fonctionnalités](#) incluent les journaux d'audit Kubernetes, l'activité de connexion RDS, les événements de AWS CloudTrail données pour Amazon S3, les volumes Amazon EBS, la surveillance du temps d'exécution et les journaux d'activité réseau Lambda. L'utilisation de ces sources de données et de ces fonctionnalités (si elles sont activées) GuardDuty génère des résultats de sécurité pour votre compte.

Une fois que vous l'avez activé GuardDuty, il commence à surveiller votre compte pour détecter les menaces potentielles en fonction des activités des sources de données de base. Par défaut, [Détection étendue des menaces](#) est activé pour tous ceux Comptes AWS qui l'ont activé GuardDuty. Cette fonctionnalité détecte les séquences d'attaque en plusieurs étapes qui couvrent plusieurs sources de données, AWS ressources et délais fondamentaux de votre compte. Pour détecter les menaces potentielles visant des AWS ressources spécifiques, vous pouvez choisir d'activer des plans de protection axés sur les cas d'utilisation qui GuardDuty offrent. Pour plus d'informations, consultez [Caractéristiques de GuardDuty](#).

Il n'est pas nécessaire d'activer explicitement l'une des sources de données de base. Lorsque vous activez S3 Protection, vous n'avez pas besoin d'activer explicitement la journalisation des événements de données Amazon S3. De même, lorsque vous activez la protection EKS, vous n'avez pas besoin d'activer explicitement les journaux d'audit Amazon EKS. Amazon GuardDuty extrait des flux de données indépendants directement à partir de ces services.

Pour un nouveau GuardDuty compte, certains des types de protection disponibles pris en charge dans un Région AWS sont activés et inclus par défaut dans la période d'essai gratuite de 30 jours. Vous pouvez choisir de toutes les refuser ou seulement l'une d'entre elles. Si vous avez déjà GuardDuty activé Compte AWS un plan de protection, vous pouvez choisir d'activer tout ou partie des plans de protection disponibles dans votre région. Pour un aperçu des plans de protection et des plans de protection qui seront activés par défaut, voir [Tarification en GuardDuty](#).

Lors de l'activation GuardDuty, tenez compte des points suivants :

- GuardDuty est un service régional, ce qui signifie que toutes les procédures de configuration que vous suivez sur cette page doivent être répétées dans chaque région que vous souhaitez surveiller GuardDuty.

Nous vous recommandons vivement de l'activer GuardDuty dans toutes les AWS régions prises en charge. Cela permet GuardDuty de générer des informations sur des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Cela permet également GuardDuty de surveiller les AWS CloudTrail événements pour les AWS services mondiaux tels que l'IAM. S'il n' GuardDuty est pas activé dans toutes les régions prises en charge, sa capacité à détecter les activités impliquant des services internationaux est réduite. Pour une liste complète des régions où cette GuardDuty offre est disponible, voir [Régions et points de terminaison](#).

- Tout utilisateur disposant de privilèges d'administrateur sur un AWS compte peut l'activer. Toutefois GuardDuty, conformément à la meilleure pratique de sécurité du privilège minimal, il est recommandé de créer un rôle, un utilisateur ou un groupe IAM à gérer GuardDuty spécifiquement. Pour plus d'informations sur les autorisations requises pour l'activation, GuardDuty consultez [Autorisations requises pour activer GuardDuty](#).
- Lorsque vous l'activez GuardDuty pour la première fois Région AWS, par défaut, tous les types de protection disponibles pris en charge dans cette région sont également activés, y compris la protection contre les logiciels malveillants pour EC2. GuardDuty crée un rôle lié à un service pour votre compte appelé. `AWSServiceRoleForAmazonGuardDuty` Ce rôle inclut les autorisations et les politiques de confiance qui permettent de GuardDuty consommer et d'analyser les événements directement à partir du [GuardDuty sources de données de base](#) pour générer des résultats de sécurité. Malware Protection for EC2 crée un autre rôle lié à un service pour votre compte

appelé. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Ce rôle inclut les autorisations et les politiques de confiance qui permettent à Malware Protection for EC2 d'effectuer des analyses sans agent afin de détecter les logiciels malveillants dans votre GuardDuty compte. Il permet GuardDuty de créer un instantané du volume EBS dans votre compte et de partager cet instantané avec le compte de GuardDuty service. Pour plus d'informations, consultez [Service-linked autorisations de rôle pour GuardDuty](#). Pour de plus amples informations sur les rôles liés à un service, veuillez consulter [Utilisation des rôles liés à un service](#).

- Lorsque vous l'activez GuardDuty pour la première fois dans une région, votre AWS compte est automatiquement inscrit à un essai GuardDuty gratuit de 30 jours pour cette région.

La vidéo suivante explique comment démarrer avec un compte administrateur GuardDuty et comment l'activer dans plusieurs comptes membres.

[Mise en route : activation d'Amazon GuardDuty pour les environnements autonomes ou à comptes multiples](#)

Étape 1 : activer Amazon GuardDuty

La première étape pour l'utiliser GuardDuty est de l'activer dans votre compte. Une fois activé, GuardDuty il commencera immédiatement à surveiller les menaces de sécurité dans la région actuelle.

Si vous souhaitez gérer les GuardDuty résultats d'autres comptes au sein de votre organisation en tant qu' GuardDuty administrateur, vous devez ajouter des comptes membres et GuardDuty les activer également.

Note

Si vous souhaitez activer la protection contre les GuardDuty programmes malveillants pour S3 sans l'activer GuardDuty, reportez-vous à la section [GuardDuty Protection contre les logiciels malveillants pour S3](#).

Standalone account environment

1. Ouvrez la GuardDuty console à <https://console.aws.amazon.com/guardduty/>
2. Sélectionnez l'option Amazon GuardDuty - Toutes les fonctionnalités.
3. Choisissez Démarrer.
4. Sur la GuardDuty page Bienvenue, consultez les conditions de service. Sélectionnez Activer GuardDuty.

Multi-account environment

Important

Pour ce processus, vous devez faire partie de la même organisation que tous les comptes que vous souhaitez gérer et avoir accès au compte de AWS Organizations gestion afin de déléguer un administrateur GuardDuty au sein de votre organisation. Des autorisations supplémentaires peuvent être nécessaires pour déléguer un administrateur. Pour plus d'informations, veuillez consulter [Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué](#).

Pour désigner un compte d' GuardDuty administrateur délégué

1. Ouvrez la AWS Organizations console à l'adresse <https://console.aws.amazon.com/organizations/>, à l'aide du compte de gestion.
2. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Est-ce GuardDuty déjà activé dans votre compte ?

- Si GuardDuty ce n'est pas déjà fait, vous pouvez sélectionner Commencer, puis désigner un administrateur GuardDuty délégué sur la GuardDuty page Bienvenue.
 - Si cette option GuardDuty est activée, vous pouvez désigner un administrateur GuardDuty délégué sur la page Paramètres.
3. Entrez l'identifiant de AWS compte à douze chiffres du compte que vous souhaitez désigner comme administrateur GuardDuty délégué de l'organisation et choisissez Déléguer.

 Note

Si GuardDuty ce n'est pas déjà fait, la désignation d'un administrateur délégué sera activée GuardDuty pour ce compte dans votre région actuelle.

Pour ajouter un compte membre

Cette procédure couvre l'ajout de comptes de membres à un compte d'administrateur GuardDuty délégué via AWS Organizations. Il est également possible d'ajouter des membres sur invitation. Pour en savoir plus sur les deux méthodes d'association de membres GuardDuty, consultez [Gérer plusieurs comptes sur Amazon GuardDuty](#).

1. Connexion au compte administrateur délégué
2. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
3. Dans le panneau de navigation, choisissez Settings (Paramètres), puis Accounts (Comptes).

La table des comptes répertorie tous les comptes de l'organisation.

4. Choisissez les comptes que vous souhaitez ajouter en tant que membres en cochant la case située à côté de l'ID du compte. Ensuite, dans le menu Action, sélectionnez Ajouter un membre.

 Tip

Vous pouvez automatiser l'ajout de nouveaux comptes en tant que membres en activant cette Auto-enablefonctionnalité ; toutefois, cela ne s'applique qu'aux comptes qui rejoignent votre organisation une fois la fonctionnalité activée.

Étape 2 : générer des exemples de résultats et explorer les opérations de base

Lorsqu'il GuardDuty découvre un problème de sécurité, il génère une constatation. Une GuardDuty constatation est un ensemble de données contenant des informations relatives à ce problème de sécurité unique. Les détails du résultat peuvent être utilisés pour vous aider à examiner le problème.

GuardDuty permet de générer des exemples de résultats à l'aide de valeurs d'espace réservé, qui peuvent être utilisées pour tester les GuardDuty fonctionnalités et vous familiariser avec les résultats avant de devoir répondre à un véritable problème de sécurité découvert par GuardDuty. Suivez le guide ci-dessous pour générer des exemples de résultats pour chaque type de recherche disponible dans GuardDuty. Pour découvrir d'autres méthodes de génération d'échantillons de résultats, notamment la génération d'un événement de sécurité simulé dans votre compte, voir [Exemples de résultats](#).

Pour créer et explorer des exemples de résultats

1. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
2. Sur la page Settings, sous Sample findings, choisissez Generate sample findings.
3. Dans le volet de navigation, choisissez Résumé pour afficher les informations relatives aux résultats générés dans votre AWS environnement. Pour de plus amples informations sur les composants du tableau de bord récapitulatif, veuillez consulter [Tableau de bord récapitulatif sur Amazon GuardDuty](#).
4. Dans le volet de navigation, choisissez Conclusions. Les exemples de résultats sont affichés sur la page Résultats actuels avec le préfixe [SAMPLE].
5. Sélectionnez un résultat dans la liste pour en afficher les détails.
 - Vous pouvez consulter les différents champs d'informations disponibles dans le volet des informations du résultat. Les différents types de résultat peuvent avoir différents champs.

Pour de plus amples informations sur les champs disponibles dans tous les types de résultat, veuillez consulter [Détails d'un résultat](#). Depuis le volet des détails, vous pouvez effectuer les actions suivantes :

- Sélectionnez l'ID du résultat en haut du volet pour ouvrir les détails JSON complets du résultat. Le fichier JSON complet peut également être téléchargé à partir de ce panneau. Le JSON contient des informations supplémentaires non incluses dans la vue de la console et est le format qui peut être ingéré par d'autres outils et services.
- Veuillez consulter la section Ressource affectée. En cas de véritable découverte, les informations présentées ici vous aideront à identifier une ressource de votre compte qui devrait faire l'objet d'une enquête et incluront des liens vers les ressources appropriées Console de gestion AWS pour des actions.
- Sélectionnez les icônes de loupe + ou - afin de créer un filtre inclusif ou exclusif pour chaque détail. Pour plus d'informations sur la recherche de filtres, veuillez consulter [Filtrer les résultats dans GuardDuty](#).

6. Archivage de tous vos exemples de résultats

- a. Sélectionnez tous les résultats en cochant la case en haut de la liste.
- b. Désélectionnez les résultats que vous souhaitez conserver.
- c. Sélectionnez le menu Actions, puis Archiver pour masquer les exemples de résultats.

Note

Pour afficher les résultats archivés, sélectionnez Actuel, puis Archivé pour changer d'affichage des résultats.

Étape 3 : configurer l'exportation GuardDuty des résultats vers un compartiment Amazon S3

GuardDuty recommande de configurer les paramètres pour exporter les résultats, car cela vous permet d'exporter vos résultats vers un compartiment S3 pour un stockage indéfini au-delà de la période de conservation de GuardDuty 90 jours. Cela vous permet de conserver des enregistrements des résultats ou de suivre les problèmes rencontrés dans votre AWS environnement au fil du temps. GuardDuty chiffre les données de résultats dans votre compartiment S3 à l'aide de AWS Key Management Service (AWS KMS key). Pour configurer les paramètres, vous devez attribuer une

clé KMS à GuardDuty l'autorisation. Pour des étapes plus détaillées, voir [Exportation des résultats générés vers Amazon S3](#).

Pour exporter GuardDuty les résultats vers le compartiment Amazon S3

1. Attacher la politique à la clé KMS

- a. Connectez-vous à la console AWS Key Management Service (AWS KMS) Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/kms>.
- b. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
- c. Dans le panneau de navigation, choisissez Clés gérées par le client.
- d. Sélectionnez une clé KMS existante ou suivez les étapes de [création d'une clé KMS de chiffrement symétrique](#) dans le manuel du AWS Key Management Service développeur.

La région de votre clé KMS et de votre compartiment Amazon S3 doit être identique.

Copiez l'ARN de la clé dans un bloc-notes pour l'utiliser dans les étapes ultérieures.

- e. Dans la section Politique relative aux clés de votre clé KMS, choisissez Modifier. Si Basculer vers l'affichage des politiques est affiché, choisissez-le pour afficher la politique clé, puis choisissez Modifier.
- f. Copiez le bloc de politique suivant dans votre politique de clé KMS :

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

Modifiez la politique en remplaçant les valeurs suivantes mises en forme *red* dans l'exemple de stratégie :

1. *KMS key ARN* Remplacez-le par le Amazon Resource Name (ARN) de la clé KMS. Pour localiser l'ARN de la clé, consultez la section [Trouver l'ID et l'ARN de la clé](#) dans le guide du AWS Key Management Service développeur.
2. *123456789012* Remplacez-le par l' Compte AWS identifiant du GuardDuty compte qui exporte les résultats.
3. Remplacez *Region2* par l' Région AWS endroit où les GuardDuty résultats sont générés.
4. Remplacez *SourceDetectorID* par le GuardDuty compte detectorID de la région spécifique où les résultats ont été générés.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

2. Attacher une politique au compartiment Amazon S3

Si vous ne possédez pas encore de compartiment Amazon S3 dans lequel vous souhaitez exporter ces résultats, consultez la section [Création d'un compartiment](#) dans le guide de l'utilisateur Amazon S3.

- a. Effectuez les étapes décrites dans la section [Pour créer ou modifier une politique de compartiment](#) dans le guide de l'utilisateur Amazon S3, jusqu'à ce que la page Modifier la politique de compartiment apparaisse.
- b. L'exemple de politique montre comment accorder GuardDuty l'autorisation d'exporter les résultats vers votre compartiment Amazon S3. Si vous modifiez le chemin après avoir configuré les résultats de l'exportation, vous devez modifier la politique pour autoriser le nouvel emplacement.

Copiez l'exemple de politique suivant et collez-le dans l'éditeur de politique Bucket.

Si vous avez ajouté la déclaration de politique avant la déclaration finale, ajoutez une virgule avant d'ajouter cette déclaration. Assurez-vous que la syntaxe JSON de votre politique de clé KMS est valide.

Exemple de stratégie de compartiment S3

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow GetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn": "arn:aws:guardduty:us-east-2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Allow PutObject",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn": "arn:aws:guardduty:us-east-2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Deny unencrypted object uploads",
```

```

        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "aws:kms"
            }
        }
    },
    {
        "Sid": "Deny incorrect encryption header",
        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
                "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            }
        }
    },
    {
        "Sid": "Deny non-HTTPS access",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        }
    }
]

```



```
}
```

c. Modifiez la politique en remplaçant les valeurs suivantes mises en forme *red* dans l'exemple de stratégie :

1. *Amazon S3 bucket ARN* Remplacez-le par le nom de ressource Amazon (ARN) du compartiment Amazon S3. Vous trouverez l'ARN du bucket sur la page Modifier la politique du bucket de la <https://console.aws.amazon.com/s3/console>.
2. *123456789012* Remplacez-le par l' Compte AWS identifiant du GuardDuty compte qui exporte les résultats.
3. Remplacez *Region2* par l' Région AWS endroit où les GuardDuty résultats sont générés.
4. Remplacez *SourceDetectorID* par le GuardDuty compte detectorID de la région spécifique où les résultats ont été générés.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

5. Remplacez une *[optional prefix]* partie de la valeur de l'*S3 bucket ARN/[optional prefix]* espace réservé par un dossier facultatif vers lequel vous souhaitez exporter les résultats. Pour plus d'informations sur l'utilisation des préfixes, consultez la section [Organisation des objets à l'aide de préfixes](#) dans le guide de l'utilisateur Amazon S3.

Lorsque vous fournissez un emplacement de dossier facultatif qui n'existe pas encore, vous ne GuardDuty créez cet emplacement que si le compte associé au compartiment S3 est le même que le compte exportant les résultats. Lorsque vous exportez des résultats vers un compartiment S3 appartenant à un autre compte, l'emplacement du dossier doit déjà exister.

6. Remplacez-le *KMS key ARN* par le Amazon Resource Name (ARN) de la clé KMS associée au chiffrement des résultats exportés vers le compartiment S3. Pour localiser l'ARN de la clé, consultez la section [Trouver l'ID et l'ARN de la clé](#) dans le guide du AWS Key Management Service développeur.

3. Étapes de GuardDuty la console

- a. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
- b. Dans le panneau de navigation, sélectionnez Settings (Paramètres).

- c. Sur la page Paramètres, sous Options d'exportation des résultats, pour le compartiment S3, choisissez Configurer maintenant (ou Modifier, selon les besoins).
- d. Pour l'ARN du compartiment S3, entrez l'adresse **bucket ARN** à laquelle vous souhaitez envoyer les résultats. Pour consulter l'ARN du compartiment, consultez [la section Affichage des propriétés d'un compartiment S3](#) dans le guide de l'utilisateur Amazon S3.
- e. Pour l'ARN de la clé KMS, entrez le **key ARN**. Pour localiser l'ARN de la clé, voir [Trouver l'ID de clé et l'ARN de la clé](#) dans le guide du AWS Key Management Service développeur.
- f. Cliquez sur Enregistrer.

Étape 4 : configurer les alertes de GuardDuty recherche via SNS

GuardDuty s'intègre à Amazon EventBridge, qui peut être utilisé pour envoyer les données des résultats à d'autres applications et services à des fins de traitement. EventBridge Vous pouvez utiliser GuardDuty les résultats pour déclencher des réponses automatiques à vos résultats en connectant les événements de recherche à des cibles telles que AWS Lambda les fonctions, l'automatisation d'Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS), etc.

Dans cet exemple, vous allez créer une rubrique SNS qui sera la cible d'une EventBridge règle, puis vous l'utiliserez EventBridge pour créer une règle qui capture les données de GuardDuty résultats. La règle qui en résulte transmet les détails du résultat à une adresse e-mail. Pour savoir comment envoyer des résultats à Slack ou Amazon Chime, et comment modifier les types de résultat pour lesquels les alertes sont envoyées, veuillez consulter [Configurer une rubrique et un point de terminaison Amazon SNS](#).

Pour créer une rubrique SNS pour vos alertes de résultats

1. Ouvrez la console Amazon SNS à l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans le volet de navigation, choisissez Rubriques.
3. Choisissez Créer la rubrique.
4. Pour Type, sélectionnez Standard.
5. Pour Nom, saisissez **GuardDuty**.
6. Choisissez Créer la rubrique. Les détails de la rubrique pour votre nouvelle rubrique s'ouvrent.
7. Dans la section Abonnements, choisissez Créer un abonnement.
8. Pour Protocole, choisissez E-mail.

9. Pour Point de terminaison, saisissez l'adresse e-mail à laquelle vous souhaitez envoyer des notifications.
10. Choisissez Créer un abonnement.

Vous devez confirmer votre abonnement par e-mail après avoir créé l'abonnement.

11. Pour vérifier la présence d'un message d'abonnement, accédez à votre boîte de réception et, dans le message d'abonnement, sélectionnez Confirmer l'abonnement.

 Note

Pour vérifier l'état de l'e-mail de confirmation, accédez à la console SNS et choisissez Abonnements.

Pour créer une EventBridge règle permettant de saisir les GuardDuty résultats et de les mettre en forme

1. Ouvrez la EventBridge console à l'adresse <https://console.aws.amazon.com/events/>.
2. Dans le volet de navigation, sous Bus, sélectionnez Rules.
3. Choisissez Créer une règle.
4. Saisissez un nom et une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

5. Pour le bus d'événements, assurez-vous que la valeur par défaut est sélectionnée et que l'option Activer la règle sur le bus d'événements sélectionné est activée.
6. Pour Type de règle, choisissez Règle avec un modèle d'événement.
7. Choisissez Suivant.
8. Sur la page Créer un modèle d'événement, dans Source d'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
9. Dans la section Modèle d'événement, pour Méthode de création, choisissez Utiliser le formulaire de modèle.
10. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
11. Pour Service AWS , choisissez GuardDuty.
12. Pour Type d'événement, choisissez GuardDuty Finding (Résultat Amazon Macie).

13. Choisissez Suivant.
14. Pour Types de cibles, choisissez service AWS .
15. Pour Sélectionner une cible, choisissez Rubrique SNS. Pour Emplacement cible, choisissez Target dans ce compte. Pour Rubrique, choisissez le nom de la rubrique SNS que vous avez créée précédemment.
16. Développer Additional settings (Paramètres supplémentaires). Pour Configurer l'entrée cible, choisissez Transformateur d'entrée.

L'ajout d'un transformateur d'entrée formate les données de recherche JSON envoyées GuardDuty en un message lisible par l'homme.

17. Choisissez Configure input transformer (Configurer le transformateur d'entrée).
18. Dans la section Transformateur d'entrée cible, pour Chemin d'entrée, collez le code suivant :

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

19. Pour formater l'e-mail, dans Template, collez le code suivant. Lorsqu'il EventBridge fournit chaque résultat, le transformateur d'entrée insère les valeurs entre crochets, par exemple <severity> et <Finding_ID>, à partir du chemin d'entrée, de sorte que vous n'avez pas besoin de les remplacer.

```
{"message": "You have a severity <severity> GuardDuty finding type <Finding_Type> in the <region> Region.\n\nFinding Description:\n<Finding_Description>\n\nFor more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"} }
```

Important

Fournissez le modèle sous la forme d'un objet JSON sur une seule ligne, avec le message enveloppé dans une clé telle message que celle illustrée dans l'exemple précédent. \nÀ utiliser pour ajouter des sauts de ligne.

GuardDuty recherche de champs tels que ceux qui `description` peuvent contenir des caractères de contrôle non échappés, y compris des nouvelles lignes. N'utilisez aucun des formats de modèle suivants :

- Une chaîne entre guillemets
- Un modèle multiligne qui utilise des chaînes entre guillemets distinctes sur des lignes distinctes

Avec ces formats, la valeur substituée peut produire du JSON non valide. EventBridge rejette ensuite l'événement et ne délivre pas la notification.

 Note

Les abonnements par e-mail reçoivent le modèle de sortie tel quel. L'e-mail affiche donc l'objet message JSON et les sauts de ligne apparaissent tels quels `\n`. Pour les notifications formatées, transmettez la rubrique Amazon SNS à Amazon Q Developer dans des applications de chat (Slack ou Amazon Chime), ou utilisez une fonction Lambda comme cible.

20. Choisissez Confirmer.
21. Choisissez Suivant.
22. (Facultatif) Saisissez une ou plusieurs balises pour la règle. Pour plus d'informations, consultez les [EventBridge balises Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.
23. Choisissez Suivant.
24. Consultez les détails de la règle et choisissez Create rule (Créer une règle).
25. (Facultatif) Testez votre nouvelle règle en générant des exemples de résultats à l'aide du processus de l'étape 2. Vous recevrez un e-mail pour chaque exemple de résultat généré.

Étapes suivantes

Au fur et à mesure que vous continuerez à l'utiliser GuardDuty, vous comprendrez quels types de résultats sont pertinents pour votre environnement. Chaque fois que vous recevez un nouveau résultat, vous pouvez trouver des informations, notamment des recommandations de correction

concernant ce résultat, en sélectionnant En savoir plus dans la description du résultat dans le volet des détails du résultat, ou en recherchant le nom du résultat sur [GuardDuty types de recherche](#).

Les fonctionnalités suivantes vous aideront à le régler de GuardDuty manière à ce qu'il puisse fournir les résultats les plus pertinents pour votre AWS environnement :

- Pour trier facilement les résultats en fonction de critères spécifiques, tels que l'ID d'instance, l'ID de compte, le nom du compartiment S3, etc., vous pouvez créer et enregistrer des filtres dans ces filtres GuardDuty. Pour plus d'informations, consultez [Filtrer les résultats dans GuardDuty](#).
- Si vous recevez des résultats concernant le comportement attendu dans votre environnement, vous pouvez automatiquement archiver les résultats en fonction des critères que vous définissez à l'aide des [règles de suppression](#).
- Pour éviter que des résultats ne soient générés à partir d'un sous-ensemble d'adresses IP fiables, ou pour que GuardDuty les adresses IP de surveillance ne soient pas contrôlées normalement, vous pouvez configurer des adresses [IP fiables et des listes de menaces](#).

GuardDuty sources de données de base

GuardDuty utilise les sources de données de base pour détecter les communications avec des domaines et adresses IP malveillants connus, et identifier les comportements potentiellement anormaux et les activités non autorisées. Pendant le transfert entre ces sources et GuardDuty, toutes les données du journal sont cryptées. GuardDuty extrait différents champs de ces sources de journaux à des fins de profilage et de détection d'anomalies, puis supprime ces journaux.

Lorsque vous l'activez GuardDuty pour la première fois dans une région, un essai gratuit de 30 jours inclut la détection des menaces pour toutes les sources de données de base. Au cours de cet essai gratuit, vous pouvez suivre une estimation de l'utilisation mensuelle ventilée par source de données de base. En tant que compte d' GuardDuty administrateur délégué, vous pouvez consulter le coût d'utilisation mensuel estimé ventilé par compte de membre qui appartient à votre organisation et qui a été activé GuardDuty. Une fois la période d'essai de 30 jours terminée, vous pouvez AWS Billing demander des informations sur le coût d'utilisation.

Il n'y a aucun coût supplémentaire pour GuardDuty accéder aux événements et aux journaux à partir de ces sources de données fondamentales.

Une fois que vous l'avez activé GuardDuty dans votre Compte AWS, il commence automatiquement à surveiller les sources de journaux expliquées dans les sections suivantes. Vous n'avez rien d'autre à activer pour commencer GuardDuty à analyser et à traiter ces sources de données afin de générer les résultats de sécurité associés.

Rubriques

- [AWS CloudTrail événements de gestion](#)
- [Journaux de flux VPC](#)
- [Journaux de requêtes DNS de Route53 Resolver](#)

AWS CloudTrail événements de gestion

AWS CloudTrail vous fournit un historique des appels d' AWS API pour votre compte, y compris les appels d'API effectués à l' Console de gestion AWS aide AWS des SDK, des outils de ligne de commande et de certains AWS services. CloudTrail vous aide également à identifier les utilisateurs et les comptes qui ont invoqué des AWS API pour les services compatibles CloudTrail, l'adresse IP source à partir de laquelle les appels ont été appelés et l'heure à laquelle les appels ont été appelés.

Pour de plus amples informations, veuillez consulter [Présentation de AWS CloudTrail](#) dans le Guide de l'utilisateur AWS CloudTrail .

GuardDuty surveille les événements CloudTrail de gestion, également appelés événements du plan de contrôle. Ces événements fournissent un aperçu des opérations de gestion effectuées sur les ressources de votre entreprise Compte AWS.

Voici des exemples d'événements de CloudTrail gestion GuardDuty surveillés :

- Configuration de la sécurité (opérations de `AttachRolePolicy` l'API IAM)
- Configuration des règles de routage des données (opérations d'API `CreateSubnet` Amazon EC2)
- Configuration de la journalisation (opérations AWS CloudTrail `CreateTrail` d'API)

Lorsque vous l'activez GuardDuty, il commence à consommer CloudTrail des événements de gestion directement CloudTrail via un flux d'événements indépendant et dupliqué et analyse vos CloudTrail journaux d'événements.

GuardDuty ne gère pas vos CloudTrail événements et n'affecte pas vos CloudTrail configurations existantes. De même, vos CloudTrail configurations n'affectent pas la façon dont les journaux d'événements sont GuardDuty consommés et traités. Pour gérer l'accès et la rétention de vos CloudTrail événements, utilisez la console CloudTrail de service ou l'API. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#) dans le Guide de AWS CloudTrail l'utilisateur.

Comment GuardDuty gère AWS CloudTrail événements mondiaux

Pour la plupart AWS des services, les CloudTrail événements sont enregistrés Région AWS là où ils ont été créés. Pour les services internationaux tels que Gestion des identités et des accès AWS (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon et CloudFront Amazon Route 53 (Route 53), les événements ne sont générés que dans la région où ils se produisent, mais ils ont une importance mondiale.

Lorsqu'il GuardDuty utilise [des événements de service CloudTrail globaux](#) (GSE) ayant une valeur de sécurité, tels que des configurations réseau ou des autorisations utilisateur, il reproduit ces événements et les traite dans chaque région où vous les avez activés. GuardDuty Ce comportement permet de GuardDuty maintenir les profils des utilisateurs et des rôles dans chaque région, ce qui est essentiel pour détecter les événements anormaux.

 Note

En ce qui concerne les résultats générés par ces événements de service mondiaux, la valeur de la région indiquée dans le résultat peut être différente de celle de la région à l'origine de la détection. Par exemple, un résultat peut s'afficher `us-east-1` sous la forme d'une région même si GuardDuty crée la détection dans une autre région.

Nous vous recommandons d'activer GuardDuty tous les éléments Régions AWS disponibles dans votre Compte AWS. Même si aucune ressource n'est déployée dans certaines régions, l'activation GuardDuty permet de protéger votre compte contre les menaces potentielles. Les acteurs de la menace peuvent potentiellement lancer des attaques par le biais de services mondiaux (tels que IAM ou Amazon CloudFront). AWS STS Ils peuvent tenter de créer des ressources non autorisées pour exploiter des régions où votre présence est limitée. GuardDuty traite les événements de service mondiaux dans toutes les régions où vous avez activé le service, y compris les régions par défaut et celles auxquelles vous avez souscrit. Cela permet de GuardDuty détecter les activités potentiellement suspectes dans votre région Compte AWS, y compris dans les régions où vous n'utilisez pas activement les ressources.

Journaux de flux VPC

La fonctionnalité Journaux de flux VPC d'Amazon VPC capture des informations sur le trafic IP circulant vers et depuis des interfaces réseau attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) dans votre environnement AWS .

Lorsque vous l'activez GuardDuty, il commence immédiatement à analyser les données du journal des flux VPC provenant des instances Amazon EC2 de votre compte. GuardDuty consomme ces données par le biais d'un flux indépendant et dupliqué de journaux de flux. Vous n'avez pas besoin de créer ou de configurer des journaux de flux VPC dans votre compte pour accéder GuardDuty à ces données. Ce processus n'affecte pas les éventuelles configurations de journaux de flux existantes.

Protection Lambda

La protection Lambda est une amélioration facultative d'Amazon. Actuellement, la surveillance de l'activité du réseau Lambda inclut les journaux de flux Amazon VPC provenant de toutes les fonctions Lambda de votre compte, même les journaux qui n'utilisent pas de réseau VPC. Pour protéger votre fonction Lambda contre les menaces de sécurité potentielles, vous

devez configurer la protection Lambda dans votre compte. GuardDuty Pour plus d'informations, consultez [Protection Lambda](#).

[GuardDuty Surveillance du temps d'exécution](#)

Lorsque l'agent GuardDuty de sécurité est déployé sur une instance Amazon EC2 et reçoit des événements d'exécution de celle-ci, il GuardDuty ne vous facture pas l'analyse des journaux Compte AWS de flux VPC provenant de cette instance. Cela permet d'éviter le double coût d'utilisation.

GuardDuty ne gère pas vos journaux de flux et ne les rend pas accessibles dans votre compte. Pour gérer l'accès et la conservation de vos journaux de flux, vous devez configurer la fonctionnalité de journaux de flux VPC.

Journaux de requêtes DNS de Route53 Resolver

Si vous utilisez des résolveurs AWS DNS pour vos instances Amazon EC2 (paramètre par défaut), GuardDuty vous pouvez accéder aux journaux de requêtes DNS de Route53 Resolver et les traiter via les résolveurs DNS internes. AWS Si vous utilisez un autre résolveur DNS, tel qu'OpenDNS ou GoogleDNS, ou si vous configurez vos propres résolveurs GuardDuty DNS, vous ne pourrez pas accéder aux données de cette source de données et les traiter.

Lorsque vous l'activez GuardDuty, il commence immédiatement à analyser les journaux de requêtes DNS de Route53 Resolver à partir d'un flux de données indépendant. Ce flux de données est distinct des données fournies par le biais de la fonctionnalité [Journalisation des requêtes de résolveur de Route 53](#). La configuration de cette fonctionnalité n'affecte pas GuardDuty l'analyse.

Note

GuardDuty ne prend pas en charge la surveillance des journaux DNS pour les instances Amazon EC2 lancées AWS Outposts car la fonctionnalité de journalisation des Amazon Route 53 Resolver requêtes n'est pas disponible dans cet environnement.

GuardDuty Détection étendue des menaces

GuardDuty Extended Threat Detection détecte automatiquement les attaques en plusieurs étapes qui couvrent des sources de données, plusieurs types de AWS ressources et des délais, dans un Compte AWS délai. Grâce à cette fonctionnalité, il GuardDuty se concentre sur la séquence de multiples événements qu'il observe en surveillant différents types de sources de données. La détection étendue des menaces met en corrélation ces événements afin d'identifier les scénarios qui se présentent comme une menace potentielle pour votre AWS environnement, puis génère une recherche de séquence d'attaque.

Rubriques

- [Exemples de scénarios de menace liés à une séquence d'attaques](#)
- [Comment ça marche](#)
- [Mettre en place des plans de protection pour optimiser la détection des menaces](#)
- [Détection étendue des menaces dans GuardDuty la console](#)
- [Comprendre et gérer les résultats des séquences d'attaques](#)
- [Ressources supplémentaires](#)

Exemples de scénarios de menace liés à une séquence d'attaques

La détection étendue des menaces couvre les scénarios de menace impliquant une compromission liée à une mauvaise utilisation des AWS informations d'identification, à des tentatives de compromission de données dans des compartiments Amazon S3 et à la compromission de conteneurs et de ressources Kubernetes dans des clusters Amazon EKS. Une seule découverte peut englober toute une séquence d'attaque. Par exemple, la liste suivante décrit les scénarios GuardDuty susceptibles de détecter :

Exemple 1 : compromission AWS des informations d'identification et des données du compartiment Amazon S3

- Un acteur malveillant obtient un accès non autorisé à une charge de travail informatique.
- L'acteur exécute ensuite une série d'actions telles que l'escalade des privilèges et l'établissement de la persévérance.
- Enfin, l'acteur exfiltre les données d'une ressource Amazon S3.

Exemple 2 : compromission du cluster Amazon EKS

- Un acteur malveillant tente d'exploiter une application conteneur au sein d'un cluster Amazon EKS.
- L'acteur utilise ce conteneur compromis pour obtenir des jetons de compte de service privilégiés.
- L'acteur exploite ensuite ces privilèges élevés pour accéder à des secrets ou à des AWS ressources sensibles de Kubernetes via des identités de pod.

En raison de la nature des scénarios de menace associés, les GuardDuty considère tous [Types de détection de séquences d'attaques](#) comme critiques.

La vidéo suivante montre comment utiliser la détection étendue des menaces.

[Démonstration de la détection GuardDuty étendue des menaces Amazon](#)

Comment ça marche

Lorsque vous activez Amazon GuardDuty dans votre compte dans un cadre spécifique Région AWS, la détection étendue des menaces est également activée par défaut. Il n'y a aucun coût

supplémentaire associé à l'utilisation de la détection étendue des menaces. Par défaut, il met en corrélation les événements entre tous [Source de données de base](#). Toutefois, lorsque vous activez d'autres plans de GuardDuty protection, tels que S3 Protection, EKS Protection et Runtime Monitoring, cela ouvre d'autres types de détections de séquences d'attaques en élargissant la gamme des sources d'événements. Cela pourrait contribuer à une analyse plus complète des menaces et à une meilleure détection des séquences d'attaques. Pour de plus amples informations, veuillez consulter [Mettre en place des plans de protection pour optimiser la détection des menaces](#).

GuardDuty met en corrélation plusieurs événements, y compris les activités et les GuardDuty résultats de l'API. Ces événements sont appelés signaux. Parfois, certains événements peuvent survenir dans votre environnement qui, à eux seuls, ne se présentent pas comme une menace potentielle claire. GuardDuty les qualifie de signaux faibles. Grâce à la détection étendue des menaces, elle GuardDuty identifie les cas où une séquence de plusieurs actions correspond à une activité potentiellement suspecte et génère une détection de séquence d'attaque dans votre compte. Ces multiples actions peuvent inclure des signaux faibles et des GuardDuty résultats déjà identifiés dans votre compte.

Note

Lors de la mise en corrélation d'événements pour des séquences d'attaques, Extended Threat Detection ne prend pas en compte les résultats archivés, y compris ceux qui sont automatiquement archivés pour cette raison. [Règles de suppression](#) Ce comportement garantit que seuls les signaux actifs et pertinents contribuent à la détection de la séquence d'attaque. Pour vous assurer que cela ne vous affecte pas, consultez les règles de suppression existantes dans votre compte. Pour de plus amples informations, veuillez consulter [Utilisation des règles de suppression avec la détection étendue des menaces](#).

GuardDuty est également conçu pour identifier les comportements d'attaque potentiels en cours ou récents (dans un délai de 24 heures) sur votre compte. Par exemple, une attaque peut être déclenchée par l'accès involontaire d'un acteur à une charge de travail informatique. L'acteur effectuerait ensuite une série d'étapes, notamment l'énumération, l'escalade des privilèges et l'exfiltration des informations d' AWS identification. Ces informations d'identification pourraient être utilisées à des fins de compromission ou d'accès malveillant aux données.

Mettre en place des plans de protection pour optimiser la détection des menaces

La détection étendue des menaces est activée automatiquement pour tous les GuardDuty comptes, évaluant par défaut les signaux de tous les plans de protection activés sur le compte. GuardDuty [Les sources de données fondamentales](#) fournissent des signaux importants pour la détection de plusieurs séquences d'attaques. Par exemple, grâce à la détection fondamentale des menaces, GuardDuty vous pouvez identifier une séquence d'attaque potentielle à partir de l'activité de découverte des privilèges IAM sur les API Amazon S3, et détecter les modifications ultérieures du plan de contrôle S3, telles que les modifications qui rendent la politique de ressources des compartiments plus permissive. Cependant, d'autres séquences d'attaque nécessitent des signaux avancés qui ne sont disponibles que dans le cadre de plans de protection avancés tels que la surveillance de l'exécution, la protection S3 et la surveillance des journaux d'audit EKS.

Rubriques

- [Détection de séquences d'attaques dans les clusters Amazon EKS](#)
- [Détection de séquences d'attaques dans les compartiments Amazon S3](#)
- [Détection de séquences d'attaques dans les clusters Amazon ECS](#)
- [Détection de séquences d'attaque dans les groupes d'instances Amazon EC2](#)
- [Détection de séquences d'attaques impliquant des charges de travail basées sur l'IA](#)

Détection de séquences d'attaques dans les clusters Amazon EKS

GuardDuty a corrélé plusieurs signaux de sécurité dans les journaux d'audit EKS, le comportement d'exécution des processus et AWS l'activité des API afin de détecter des modèles d'attaque sophistiqués. Pour bénéficier de la détection étendue des menaces pour EKS, vous devez activer au moins l'une de ces fonctionnalités : la protection EKS ou la surveillance de l'exécution (avec le module complémentaire EKS). EKS Protection surveille les activités du plan de contrôle via des journaux d'audit, tandis que Runtime Monitoring observe les comportements au sein des conteneurs.

Pour une couverture maximale et une détection complète des menaces, GuardDuty recommande d'activer les deux plans de protection. Ensemble, ils créent une vue complète de vos clusters EKS, ce qui permet GuardDuty de détecter des modèles d'attaque complexes. Par exemple, il peut identifier un déploiement anormal d'un conteneur privilégié (détecté avec EKS Protection), suivi de tentatives de persistance, de cryptominage et de création d'un shell inversé dans ce conteneur (détecté avec Runtime Monitoring). GuardDuty représente ces événements connexes sous la forme d'un seul

résultat de gravité critique, appelé. [AttackSequence:EKS/CompromisedCluster](#) Lorsque vous activez les deux plans de protection, la détection de la séquence d'attaque couvre les scénarios de menace suivants :

- Compromis des conteneurs exécutant des applications Web vulnérables
- Accès non autorisé via des informations d'identification mal configurées
- Tentatives d'augmentation des privilèges
- Demandes d'API suspectes
- Tentatives d'accès aux données de manière malveillante

La liste suivante indique quand ces plans de protection dédiés sont activés individuellement :

Protection EKS

L'activation de la protection EKS permet GuardDuty de détecter les séquences d'attaque impliquant les activités du plan de contrôle du cluster Amazon EKS. Cela permet de GuardDuty corréliser les journaux d'audit EKS et AWS l'activité de l'API. Par exemple, GuardDuty peut détecter une séquence d'attaque dans laquelle un acteur tente d'accéder sans autorisation à des secrets de cluster, modifie les autorisations de contrôle d'accès basé sur les rôles (RBAC) de Kubernetes et crée des pods privilégiés. Pour plus d'informations sur l'activation de ce plan de protection, consultez [Protection EKS](#).

Surveillance de l'exécution pour Amazon EKS

L'activation de la surveillance de l'exécution pour les clusters Amazon EKS permet GuardDuty d'améliorer la détection des séquences d'attaques EKS grâce à une visibilité au niveau du conteneur. Cela permet de GuardDuty détecter les processus malveillants potentiels, les comportements d'exécution suspects et l'exécution potentielle de programmes malveillants. Par exemple, GuardDuty peut détecter une séquence d'attaque dans laquelle un conteneur commence à présenter un comportement suspect, tel que des processus de minage de cryptomonnaie ou l'établissement de connexions à des terminaux malveillants connus. Pour plus d'informations sur l'activation de ce plan de protection, consultez [Surveillance d'exécution](#).

Si vous n'activez pas la protection EKS ou la surveillance de l'exécution, GuardDuty vous ne pourrez pas générer de [Types de recherche de protection EKS](#) ou [Types de recherche liés à la surveillance du temps](#). Par conséquent, GuardDuty il ne sera pas en mesure de détecter des séquences d'attaque en plusieurs étapes impliquant des résultats associés.

Détection de séquences d'attaques dans les compartiments Amazon S3

L'activation de la protection S3 permet GuardDuty de détecter les séquences d'attaques impliquant des tentatives de compromission des données dans vos compartiments Amazon S3. Sans S3 Protection, GuardDuty vous pouvez détecter lorsque la politique de ressources de votre compartiment S3 devient trop permissive. Lorsque vous activez S3 Protection, il est GuardDuty en mesure de détecter les activités d'exfiltration de données potentielles susceptibles de se produire lorsque votre compartiment S3 devient trop permissif.

Si la protection S3 n'est pas activée, GuardDuty vous ne pourrez pas générer de données individuelles [Types de détection de la protection S3](#). Par conséquent, GuardDuty il ne sera pas en mesure de détecter des séquences d'attaque en plusieurs étapes impliquant des résultats associés. Pour plus d'informations sur l'activation de ce plan de protection, consultez [Protection S3](#).

Détection de séquences d'attaques dans les clusters Amazon ECS

GuardDuty peut identifier les séquences d'attaque telles que les processus malveillants, les connexions à des terminaux malveillants ou les comportements de cryptominage au sein des conteneurs ECS. En corrélant divers signaux liés à l'activité du réseau, au comportement d'exécution des processus et à l'activité des AWS API, GuardDuty vous pouvez identifier des modèles d'attaque complexes qui pourraient ne pas être détectés lors de détections individuelles et cartographier le vecteur d'attaque complet.

GuardDuty représente ces événements connexes sous la forme d'un seul résultat de gravité critique, appelé `AttackSequence:ECS/CompromisedCluster`. La détection de la séquence d'attaque couvre les scénarios de menace suivants :

- Compromis des conteneurs assurant des services vulnérables
- Exécution non autorisée d'outils suspects, de logiciels malveillants ou de processus de minage de cryptomonnaie
- Tentatives d'augmentation des privilèges
- Communication avec des terminaux suspects

Important

La détection étendue des menaces pour ECS nécessite une surveillance de l'exécution pour Fargate ou EC2, en fonction de votre type d'infrastructure ECS. Runtime Monitoring observe

les comportements au sein des conteneurs ECS exécutés à la fois sur des instances Fargate et EC2. ECS sur les instances EC2 gérées n'est pas pris en charge.

Détection de séquences d'attaque dans les groupes d'instances Amazon EC2

GuardDuty peut identifier les séquences d'attaque affectant des instances individuelles ou des groupes d'instances partageant des attributs communs tels que les groupes Auto Scaling, les profils d'instance IAM, les modèles de lancement, les CloudFormation piles, les AMI ou les ID VPC. Ces instances peuvent présenter des comportements suspects tels que des processus malveillants, des connexions à des terminaux malveillants, du minage de cryptomonnaies ou une utilisation anormale des informations d'identification des instances EC2.

La détection de la séquence d'attaque détecte les scénarios de menace suivants :

- Compromis des instances exécutant des services vulnérables
- Utilisation des informations d'identification d'instance Amazon EC2 obtenues via IMDS depuis l'extérieur du AWS compte auquel les informations d'identification ont été émises
- Utilisation en tant qu'infrastructure pour des attaques telles que le proxy, le scan ou le déni de service
- Exécution non autorisée d'outils suspects, de logiciels malveillants ou de processus de minage de cryptomonnaie
- Communication avec des terminaux suspects

La détection étendue des menaces permet d'identifier ces menaces. GuardDuty représente ces événements connexes sous la forme d'un seul résultat de gravité critique, appelé.

`AttackSequence:EC2/CompromisedInstanceGroup`

Pour améliorer la détection étendue des menaces pour les fonctionnalités de détection EC2, activez Runtime Monitoring. La combinaison de Foundational GuardDuty, qui surveille l'activité du réseau, CloudTrail et de Runtime Monitoring, qui observe le comportement des processus et les appels système au sein des instances, permet une détection des menaces plus complète. Cette surveillance intégrée permet de GuardDuty détecter des séquences d'attaques sophistiquées telles que les accès non autorisés via des informations d'identification mal configurées, les tentatives d'élévation de privilèges et les accès non autorisés à des données sensibles. En corrélant ces divers signaux, il est

GuardDuty possible d'identifier des modèles d'attaque complexes qui pourraient ne pas être détectés lors de détections individuelles et de cartographier le vecteur d'attaque complet.

Détection de séquences d'attaques impliquant des charges de travail basées sur l'IA

Activez cette option [Protection de l'IA](#) pour aider à GuardDuty détecter les séquences d'attaques qui menacent les charges de travail d'IA de votre compte. AI Protection analyse les événements AWS CloudTrail liés aux données provenant d'Amazon Bedrock et d'Amazon SageMaker AI. Il peut détecter des activités telles que les invocations anormales de modèles, les attaques visant à réduire les coûts et les tentatives d'injection directe et rapide.

Pour ajouter des signaux provenant de vos charges de travail d'IA aux séquences d'[AttackSequence:IAM/CompromisedCredentials](#)attaques, vous devez activer AI Protection. GuardDuty peut ensuite utiliser les types de résultats suivants comme signaux de corrélation :

- [Impact:IAMUser/AnomalousModelInvocation](#)
- [Impact:IAMUser/CostHarvesting](#)
- [Impact:IAMUser/PromptInjection.Direct](#)

Par exemple, un acteur malveillant peut utiliser les mêmes AWS informations d'identification potentiellement compromises pour faire une invocation anormale du modèle Amazon Bedrock ou Amazon SageMaker AI. GuardDuty peut corréler cette invocation à d'autres actions suspectes effectuées avec ces informations d'identification. Il les représente ensuite sous la forme d'une découverte de séquence d'[AttackSequence:IAM/CompromisedCredentials](#)attaque unique. À eux seuls, les résultats de AI Protection ne génèrent pas de séquence d'attaque.

Si AI Protection n'est pas activée, GuardDuty impossible de générer un individu [Types de détection de protection contre l'IA](#). Par conséquent, GuardDuty impossible de détecter les séquences d'attaque en plusieurs étapes impliquant ces résultats. Pour plus d'informations sur l'activation de ce plan de protection, consultez [Protection de l'IA](#).

Détection étendue des menaces dans GuardDuty la console

Par défaut, la page Détection étendue des menaces de la GuardDuty console affiche le statut **Activé**. Avec la détection fondamentale des menaces, le statut représente la capacité à GuardDuty

détecter une séquence d'attaque potentielle impliquant une activité de découverte de privilèges IAM sur les API Amazon S3 et la détection de modifications ultérieures du plan de contrôle S3.

Procédez comme suit pour accéder à la page de détection étendue des menaces dans GuardDuty la console :

1. Vous pouvez ouvrir GuardDuty la console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation de gauche, choisissez **Extended Threat Detection**.

Cette page fournit des détails sur les scénarios de menace couverts par la détection étendue des menaces.

3. Sur la page **Détection étendue des menaces**, consultez la section **Plans de protection associés**. Si vous souhaitez activer des plans de protection dédiés afin d'améliorer la couverture de détection des menaces sur votre compte, sélectionnez l'option **Configurer pour ce plan de protection**.

Comprendre et gérer les résultats des séquences d'attaques

Les résultats de la séquence d'attaque sont identiques GuardDuty aux autres résultats de votre compte. Vous pouvez les consulter sur la page **Résultats de la GuardDuty console**. Pour plus d'informations sur l'affichage des résultats, consultez [Page de résultats dans la GuardDuty console](#).

À l'instar des autres GuardDuty résultats, les résultats de la séquence d'attaque sont également automatiquement envoyés à Amazon EventBridge. En fonction de vos paramètres, les résultats des séquences d'attaques sont également exportés vers une destination de publication (compartiment Amazon S3). Pour définir une nouvelle destination de publication ou mettre à jour une destination existante, consultez [Exportation des résultats générés vers Amazon S3](#).

Ressources supplémentaires

Consultez les sections suivantes pour mieux comprendre les séquences d'attaques :

- Après avoir découvert la détection étendue des menaces et les séquences d'attaque, vous pouvez générer des exemples de types de détection de séquences d'attaque en suivant les étapes décrites dans [Exemples de résultats](#).
- En savoir plus sur [Types de détection de séquences d'attaques](#).

- Passez en revue les résultats et explorez les détails des résultats associés à [Détails de recherche de la séquence d'attaque](#).
- Hiérarchisez et traitez les types de détection de séquences d'attaques en suivant les étapes correspondant aux ressources affectées associées dans [Correction des résultats](#).

Configuration des plans de protection

La page Plans de protection de la GuardDuty console regroupe toutes les configurations des plans de protection sur une seule page. Vous pouvez activer ou désactiver les plans de protection, configurer les paramètres d'activation automatique pour les AWS Organizations comptes et consulter les statistiques des comptes des membres à partir d'un seul endroit.

Présentation de

La page des plans de protection unifiés évite d'avoir à accéder aux pages des plans de protection individuels pour la configuration. La navigation de la console affiche un seul lien vers les plans de protection.

La page affiche les plans de protection dans l'ordre suivant :

1. Fondateur GuardDuty — Activez ou désactivez GuardDuty et configurez l'activation automatique pour les AWS Organizations comptes.
2. Protection S3 — Surveillez les événements liés aux données Amazon S3 pour détecter les menaces potentielles qui pèsent sur vos données.
3. Surveillance de l'exécution : surveillez les événements au niveau du système d'exploitation pour les charges de travail EKS, ECS et EC2.
4. Journaux d'audit EKS — Surveillez les journaux d'audit Amazon EKS pour détecter les menaces potentielles qui pèsent sur vos clusters.
5. Protection RDS — Surveillez l'activité de connexion RDS pour détecter les menaces potentielles qui pèsent sur vos bases de données.
6. Protection Lambda — Surveillez l'activité du réseau des fonctions Lambda pour détecter les menaces potentielles.

Chaque plan de protection affiche les informations suivantes :

- État de la fonctionnalité (activé ou non activé)
- Auto-enable statut des AWS Organizations comptes
- AWS Organizations statistiques des membres des comptes

Configuration de tous les plans de protection

Pour configurer les plans de protection à partir de la page unifiée, procédez comme suit :

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Tous les conteneurs de plans de protection passent en mode édition.
4. Apportez des modifications à l'un ou à l'ensemble des plans de protection. Pour chaque plan, vous pouvez activer ou désactiver la fonctionnalité et configurer le paramètre d'activation automatique pour les comptes de l'organisation.
5. Choisissez Tout enregistrer. Un mode de confirmation apparaît résumant toutes les modifications, y compris le nom de la fonctionnalité, le statut et la valeur d'activation automatique pour chaque plan modifié.
6. Passez en revue les modifications, choisissez Confirmer et enregistrez. Toutes les modifications sont enregistrées par lots.

Auto-enable options

Chaque plan de protection fournit les options d'activation automatique suivantes pour les comptes d'entreprise :

Activer pour tous les comptes

Activez cette fonctionnalité pour tous les GuardDuty comptes actifs de l'organisation. Cela inclut les nouveaux comptes qui rejoignent l'organisation.

Activer les nouveaux comptes

Cela s'appliquera à tous les nouveaux comptes lorsqu'ils seront ajoutés à l'organisation.

Ne pas activer automatiquement

La fonctionnalité n'est pas automatiquement activée pour les comptes d'organisation.

Pour le GuardDuty conteneur de base, les options d'activation automatique utilisent AWS Organizations un libellé spécifique :

- Activer pour tous les AWS Organizations comptes — Activez GuardDuty pour tous les comptes actifs de votre AWS Organizations.
- Activer les nouveaux AWS Organizations comptes — Cela s'appliquera à tous les nouveaux comptes lorsqu'ils seront ajoutés à votre AWS Organizations.

Configuration de la surveillance de l'exécution

Le conteneur Runtime Monitoring possède une structure parent-enfant avec les sous-fonctionnalités suivantes :

- Surveillance du temps d'exécution (EKS)
- Surveillance du temps d'exécution (ECS)
- Surveillance du temps d'exécution (EC2)

Le paramètre Runtime Monitoring Infrastructure est affiché dans une section extensible. Ce paramètre est nécessaire au fonctionnement de la surveillance du temps d'exécution pour EKS, ECS et EC2, mais ne fournit pas de protection à lui seul.

Contraintes bidirectionnelles

Les sous-fonctionnalités et l'infrastructure de surveillance du temps d'exécution ont les relations suivantes :

Activer une sous-fonctionnalité

Active automatiquement l'infrastructure de surveillance du temps d'exécution si elle a été désactivée.

Désactiver une sous-fonctionnalité

Aucun effet sur l'infrastructure de surveillance du temps d'exécution.

Activer l'infrastructure de surveillance du temps d'exécution

Aucun effet sur les sous-fonctionnalités.

Désactiver l'infrastructure de surveillance de l'exécution

Désactive toutes les sous-fonctionnalités.

Pour les paramètres d'activation automatique, les contraintes suivantes s'appliquent :

Augmenter l'activation automatique d'une sous-fonctionnalité

L'infrastructure de surveillance du temps d'exécution est toujours égale au maximum de toutes les sous-fonctionnalités.

Réduire l'activation automatique d'une sous-fonctionnalité

L'infrastructure de surveillance du temps d'exécution recalcule en fonction du nouveau maximum de toutes les sous-fonctionnalités.

Augmentez l'activation automatique de l'infrastructure de surveillance des temps d'exécution

Aucun effet sur les sous-fonctionnalités.

Activation automatique de l'infrastructure de surveillance à faible temps d'exécution

Réduit toute sous-fonctionnalité qui dépasse la nouvelle valeur parent pour qu'elle corresponde à celle-ci.

Note

Un avertissement s'affiche lorsqu'une sous-fonctionnalité a une valeur différente de celle de l'infrastructure de surveillance du temps d'exécution (incompatibilité ou activation automatique). L'activation de l'infrastructure de surveillance du temps d'exécution uniquement vous place en mode manuel sans gestion automatique de l'agent de sécurité. Activez la surveillance du temps d'exécution pour EKS, ECS ou EC2 afin de gérer automatiquement l'agent de sécurité pour vos charges de travail.

Statistiques de l'organisation

Chaque conteneur de plan de protection affiche les statistiques des comptes des membres indiquant le nombre de comptes sur lesquels cette fonctionnalité est activée. Lorsque les statistiques de l'organisation ne sont pas encore disponibles (par exemple, dans les 24 heures suivant l'activation), la page affiche un indicateur de statut en attente accompagné d'un message expliquant que des statistiques sont collectées.

Intégration de la page des comptes

Le bouton Modifier dans la section d'activation automatique de la page Comptes vous redirige vers la page Plans de protection au lieu d'ouvrir l'ancien mode de configuration.

GuardDuty Protection de l'IA

GuardDuty AI Protection étend la détection des GuardDuty menaces Amazon aux charges de travail basées sur AWS l'IA. Lorsque vous activez la protection par IA, elle GuardDuty analyse les événements liés aux AWS CloudTrail données d'Amazon Bedrock, Amazon Bedrock AgentCore et Amazon SageMaker AI, ainsi que les événements de AWS CloudTrail gestion. GuardDuty utilise ces données pour détecter les activités potentiellement suspectes qui ciblent les modèles de base et les applications qui les invoquent. Lorsqu'il GuardDuty identifie une menace potentielle, il en génère une ou plusieurs [Types de détection de protection contre l'IA](#).

Lorsque vous activez la protection par IA, vous GuardDuty pouvez détecter les types de menaces suivants :

- Invocations anormales des modèles Amazon Bedrock ou SageMaker Amazon AI qui s'écartent de la base de référence établie pour une identité ou un compte, telles que les invocations provenant d'une adresse IP inhabituelle, d'une API inhabituelle ou d'un modèle inhabituel.
- Attaques de collecte des coûts, dans lesquelles un acteur malveillant envoie des données informatiques coûteuses à un modèle Amazon Bedrock ou Amazon SageMaker AI pour augmenter la consommation de jetons et les coûts d'exploitation du compte.
- Tentatives d'injection directe, dans lesquelles un acteur malveillant crée une invite malveillante pour obliger un modèle de base à ignorer ses instructions d'origine. Cette détection nécessite Amazon Bedrock Guardrails et ne s'applique qu'aux charges de travail Amazon Bedrock.

Note

Les types de recherche qui GuardDuty peuvent être générés dans et Région AWS dépendent des services d'IA disponibles dans cette région :

- Les types [Impact:IAMUser/AnomalousModelInvocation](#) de [Impact:IAMUser/CostHarvesting](#) recherche et de recherche nécessitent Amazon Bedrock ou Amazon SageMaker AI. Dans les régions où Amazon Bedrock n'est pas disponible, GuardDuty génère ces types de recherche uniquement à partir des invocations du modèle Amazon SageMaker AI.
- Le type de [Impact:IAMUser/PromptInjection.Direct](#) recherche nécessite Amazon Bedrock Guardrails. Il n'est pas disponible dans les régions où Amazon Bedrock Guardrails n'est pas pris en charge.

Pour la liste des régions dans lesquelles chaque type de recherche est pris en charge, voir [Region-specific disponibilité des fonctionnalités](#).

 Tip

Pour tirer le meilleur parti de la protection contre l'intelligence artificielle, utilisez Amazon Bedrock Guardrails pour lancer des attaques rapides sur tous les comptes de votre entreprise. AWS Utilisez les [politiques AWS Organizations d'Amazon Bedrock](#) pour gérer ces paramètres de garde-corps de manière centralisée. Cela permet une protection uniforme sur tous les comptes grâce à un contrôle et une gestion centralisés. Lorsqu'un garde-corps d'attaque rapide est appliqué, GuardDuty cela crée des résultats d'injection rapides. Pour plus d'informations, consultez [Impact:IAMUser/PromptInjection.Direct](#).

Pour détecter les menaces qui pèsent sur vos charges de travail basées sur l'IA, vous devez activer la protection par IA dans votre GuardDuty compte. Pour plus d'informations sur l'activation de la protection par IA, voir [Activation de la protection par l'IA dans les environnements à comptes multiples](#) pour les environnements à comptes multiples ou. [Activation de la protection par l'IA pour un compte autonome](#)

Rubriques

- [Comment fonctionne la protection par IA](#)
- [Tarification de la protection de l'IA](#)
- [Détections de menaces supplémentaires pour les charges de travail liées à l'IA](#)
- [Activation de la protection par l'IA dans les environnements à comptes multiples](#)
- [Activation de la protection par l'IA pour un compte autonome](#)

Comment fonctionne la protection par IA

Lorsque vous activez la protection par IA pour un compte ou pour l'ensemble de votre organisation, la collecte d'événements de AWS CloudTrail données à partir des services d'IA dans les comptes surveillés commence GuardDuty automatiquement. Vous n'avez pas besoin de créer une trace,

d'activer l'enregistrement des événements de données ou d'apporter des modifications à vos applications d'IA.

Pour collecter les données relatives aux événements, GuardDuty crée un [canal AWS CloudTrail lié au service](#) dans chaque compte surveillé. Le canal lié au service diffuse les événements de AWS CloudTrail données pour Amazon Bedrock, Amazon Bedrock AgentCore et Amazon SageMaker AI, ainsi que les ressources d'IA associées à des fins d'analyse. GuardDuty Parce que GuardDuty crée et gère ce canal :

- GuardDuty configure les paramètres des événements de données de la chaîne, et le propriétaire du compte ne peut pas les modifier. Cela signifie que la détection des menaces ne dépend pas de la configuration ou de la gestion d'une trace par le propriétaire du compte.
- Chaque compte surveillé peut confirmer que le canal est actif dans la CloudTrail console (sous Paramètres, Service-linkedcanaux) ou en appelant l'opération AWS CloudTrail [ListChannelsAPI](#).

GuardDuty utilise deux méthodes de détection pour générer des résultats de protection contre l'IA, en fonction du type de détection :

- Pour les types [Impact:IAMUser/AnomalousModelInvocation](#) et la [Impact:IAMUser/CostHarvesting](#) recherche, GuardDuty utilise un modèle d'apprentissage automatique (ML) de détection d'anomalies pour analyser les événements collectés et établir une base de référence pour l'activité d'invocation normale du modèle pour chaque identité IAM et. Compte AWS GuardDuty génère un résultat lorsqu'il détecte une activité qui s'écarte de manière significative de cette base de référence.
- Pour le type de [Impact:IAMUser/PromptInjection.Direct](#) recherche, GuardDuty génère une constatation lorsqu'Amazon Bedrock Guardrails évalue une invite et détecte une attaque rapide, en fonction de l'événement de données qui en résulte. AWS CloudTrail

Pour plus d'informations sur les événements AWS CloudTrail liés aux données, consultez la section [Enregistrement des événements liés aux données](#) dans le Guide de AWS CloudTrail l'utilisateur.

Tarification de la protection de l'IA

Lorsque vous activez GuardDuty AI Protection, les GuardDuty frais sont calculés en fonction du volume d'événements de AWS CloudTrail données analysés, mesuré en Go. GuardDuty crée le canal lié au service sans CloudTrail frais supplémentaires pour vous. Le coût de la collecte de

ces événements de données est inclus dans le coût d'utilisation de AI Protection. Vous continuez également à payer des frais d'utilisation standard pour GuardDuty tout autre plan de protection activé. Pour consulter les tarifs actuels et des exemples, consultez [GuardDuty les tarifs Amazon](#).

Détections de menaces supplémentaires pour les charges de travail liées à l'IA

Outre le plan de protection de l'IA, les plans Amazon GuardDuty Foundational et [Lambda](#) Protection proposent des détections pour vous aider à sécuriser et à détecter les menaces qui pèsent sur les charges de travail basées sur l'IA. AWS

[Le plan de GuardDuty base surveille les événements AWS CloudTrail de gestion afin de détecter les activités suspectes et malveillantes dans les charges de travail d'IA créées à l'aide de AWS services tels qu'Amazon Bedrock et Amazon AI. SageMaker](#) Par exemple, GuardDuty peut identifier des activités telles que :

- Suppression inhabituelle des rambardes de sécurité Amazon Bedrock
- Modification d'une source de données d'entraînement du modèle susceptible de provoquer une attaque d'empoisonnement des données
- Journalisation désactivée pour les invocations du modèle Amazon Bedrock susceptibles d'indiquer des tentatives d'échapper à la détection
- Instance de bloc-notes inhabituelle ou création de postes de formation dans Amazon SageMaker AI
- Informations d'identification Amazon Elastic Compute Cloud exfiltrées qui auraient pu être utilisées pour appeler des API dans Amazon Bedrock, Amazon SageMaker AI ou des charges de travail d'IA autogérées sur des instances Amazon EC2, des clusters Amazon EKS ou des tâches Amazon ECS.

GuardDuty Lambda Protection peut aider à détecter les menaces potentielles liées aux agents Amazon Bedrock. Cela peut inclure des activités réseau suspectes telles que le minage de cryptomonnaies et des communications avec des serveurs de commande et de contrôle malveillants. Ces menaces peuvent être causées par une attaque de la chaîne d'approvisionnement ou par des incitations complexes.

Activation de la protection par l'IA dans les environnements à comptes multiples

Dans un environnement à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la protection par l'IA pour les comptes des membres de l'organisation. Les comptes membres ne peuvent pas modifier cette configuration à partir de leurs propres comptes. Le compte d' GuardDuty administrateur délégué gère les comptes des membres à l'aide AWS Organizations de la protection par IA et peut choisir d'activer automatiquement la protection par IA pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements à comptes multiples, consultez [Gérer plusieurs comptes sur Amazon](#). GuardDuty

Activation de la protection AI pour le compte GuardDuty d'administrateur délégué

Choisissez votre méthode d'accès préférée pour activer la protection AI pour le compte GuardDuty d'administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Sous Protection AI, vous pouvez consulter l'état de configuration actuel de AI Protection.
4. Effectuez l'une des actions suivantes :

Utilisation Activer pour tous les comptes

- Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
- Cliquez sur Enregistrer.

Utilisation Configuration manuelle des comptes

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Cliquez sur Enregistrer.

API/CLI

Exécutez l'opération d'API [UpdateDetector](#) en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features name` en tant que `AI_PROTECTION` et `status` en tant que `ENABLED` ou `DISABLED`.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active la protection AI pour le compte GuardDuty d'administrateur délégué. `12abc34d567e8fa901bc2d34e56789f0` Remplacez-le par l'identifiant du détecteur de votre compte et `us-east-1` par la région dans laquelle vous souhaitez activer la protection par IA.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Pour désactiver la protection AI, remplacez `ENABLED` par `DISABLED`.

Activation de la protection par l'IA pour tous les comptes de membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la protection par l'IA pour tous les comptes de membres actifs existants de l'organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Sous Protection contre l'IA, dans la section Comptes membres actifs, sélectionnez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Cliquez sur Enregistrer.

API/CLI

Pour activer ou désactiver de manière sélective la protection par l'IA pour vos comptes membres, exécutez l'opération d'[UpdateMemberDetectors](#) API en utilisant la votre *detector ID*.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active la protection AI pour un seul compte membre. Pour la désactiver, remplacez ENABLED par DISABLED. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --region us-east-1 --features '[{"Name":
"AI_PROTECTION", "Status": "ENABLED"}]'
```

Lorsque la commande s'exécute correctement, elle renvoie une liste vide deUnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, la réponse indique cet identifiant de compte ainsi qu'un résumé du problème.

Auto-enable Protection par l'IA pour les nouveaux comptes de membres

Choisissez votre méthode d'accès préférée pour activer la protection par l'IA pour les nouveaux comptes qui rejoignent votre organisation.

Dans la console, le compte GuardDuty administrateur délégué peut activer automatiquement la protection AI pour les nouveaux comptes membres en utilisant la page Plans de protection ou la page Comptes.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :
 - À l'aide de la page Plans de protection :

1. Dans le volet de navigation, sélectionnez Plans de protection.
 2. Choisissez Configurer toutes les activations.
 3. Sous Protection contre l'intelligence artificielle, choisissez Configurer les comptes manuellement, puis sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la protection AI est GuardDuty automatiquement activée pour ce compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
 4. Cliquez sur Enregistrer.
- Utilisation de la page Comptes :
 1. Dans le panneau de navigation, choisissez Accounts (Comptes).
 2. Sur la page Comptes, sélectionnez Auto-enablePréférences.
 3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous AI Protection.
 4. Cliquez sur Enregistrer.

API/CLI

Pour activer la protection par l'IA pour les nouveaux comptes membres, exécutez l'opération [UpdateOrganizationConfiguration](#) d'API en utilisant le vôtre *detector ID*.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active la protection par l'IA pour les nouveaux comptes qui rejoignent votre organisation. Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes, définissez `AutoEnable` sur `NONE`.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features '[{"Name": "AI_PROTECTION", "AutoEnable": "NEW"}]'
```

Activation de la protection par l'IA pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection sur son AWS compte dans une région spécifique.

Si votre compte est associé à un compte GuardDuty administrateur via AWS Organizations ou sur invitation, cette section ne s'applique pas à vous. Pour plus d'informations sur la gestion de plusieurs comptes, consultez [Activation de la protection par l'IA dans les environnements à comptes multiples](#).

Une fois que vous avez activé la protection par IA, GuardDuty commence à surveiller l'activité d'invocation d'Amazon Bedrock et du modèle Amazon SageMaker AI qu'elle collecte CloudTrail pour votre compte.

Choisissez votre méthode d'accès préférée pour activer la protection AI dans votre compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le sélecteur de région situé dans le coin supérieur droit, sélectionnez la région dans laquelle vous souhaitez activer la protection par l'IA.
3. Dans le volet de navigation, sélectionnez Plans de protection.
4. Choisissez Configurer toutes les activations. Sous Protection de l'IA, choisissez Activer pour activer la protection de l'IA.
5. Choisissez Enregistrer tout, puis cliquez sur Confirmer et enregistrez.

API/CLI

Exécutez l'opération [UpdateDetector](#) API en utilisant votre propre identifiant de détecteur régional et en transmettant l'featuresobjet name sous AI_PROTECTION et en status tant queENABLED.

Vous pouvez également utiliser le AWS CLI pour activer la protection par IA. Exécutez la commande suivante et remplacez-la **12abc34d567e8fa901bc2d34e56789f0** par l'ID du détecteur de votre compte et **us-east-1** par la région dans laquelle vous souhaitez activer la protection par IA.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Pour désactiver la protection AI, remplacez ENABLED parDISABLED.

GuardDuty Protection EKS

Note

Vous pouvez configurer EKS Protection ainsi que tous les autres plans de protection à partir d'une seule page de la GuardDuty console. Pour de plus amples informations, veuillez consulter [Configuration des plans de protection](#).

EKS Protection vous aide à détecter les risques de sécurité potentiels dans les clusters Amazon Elastic Kubernetes Service (Amazon EKS) de votre environnement. AWS Par exemple, il vous aide à détecter les accès à un cluster EKS mal configuré par un acteur non authentifié qui tente de collecter des secrets ou des AWS informations d'identification auprès de votre cluster. EKS Protection utilise les journaux d'audit EKS pour analyser les activités des utilisateurs et des applications.

Lorsque vous activez la protection EKS, commence GuardDuty automatiquement à surveiller vos clusters Amazon EKS pour détecter les menaces de sécurité potentielles. GuardDuty utilise son propre flux indépendant pour collecter et analyser ; [Journaux d'audit EKS dans EKS Protection](#) aucune configuration supplémentaire n'est requise.

Lorsqu'une menace potentielle est GuardDuty détectée sur la base de la surveillance du journal d'audit EKS, elle génère un constat de sécurité. Pour plus d'informations sur les types de recherche GuardDuty susceptibles d'être générés lorsque vous activez la protection EKS, consultez [Types de recherche de protection EKS](#).

Note

Pour consulter les journaux d'audit EKS dans votre compte (facultatif), vous pouvez configurer la journalisation du plan de contrôle Amazon EKS pour envoyer les journaux d'audit à CloudWatch Logs. Cette configuration est distincte de la protection EKS et n'est pas requise pour la fonctionnalité de surveillance de la sécurité dans GuardDuty.

essai gratuit de 30 jours

- Lorsque vous activez GuardDuty in an Compte AWS in an Région AWS pour la première fois, vous bénéficiez d'un essai gratuit de 30 jours. Dans ce cas, GuardDuty vous activerez également EKS Protection, qui est incluse dans l'essai gratuit de 30 jours.

- Lorsque vous utilisez déjà EKS Protection GuardDuty et décidez de l'activer pour la première fois, votre compte dans cette région bénéficiera d'un essai gratuit de 30 jours pour EKS Protection.
- Vous pouvez choisir de désactiver la protection EKS dans n'importe quelle région à tout moment.
- Au cours de l'essai gratuit de 30 jours, vous pouvez obtenir une estimation de vos coûts d'utilisation pour ce compte et cette région. Après la fin de l'essai gratuit de 30 jours, la protection EKS GuardDuty ne sera pas automatiquement désactivée. Votre compte dans cette région commencera à entraîner des frais d'utilisation. Pour de plus amples informations, veuillez consulter [Surveillance de l'utilisation et estimation des coûts](#).

Lorsque vous désactivez la protection EKS, la surveillance et l'analyse des journaux d'audit EKS de vos ressources Amazon EKS sont GuardDuty immédiatement arrêtées.

Il est possible que la protection EKS ne soit pas disponible partout Régions AWS où GuardDuty elle est disponible. Pour de plus amples informations, veuillez consulter [Region-specific disponibilité des fonctionnalités](#).

 Note

EKS Runtime Monitoring est géré dans le cadre de Runtime Monitoring. Pour de plus amples informations, veuillez consulter [GuardDuty Surveillance du temps d'exécution](#).

Journaux d'audit EKS dans EKS Protection

Les journaux d'audit EKS capturent les actions séquentielles au sein de votre cluster Amazon EKS, notamment les activités des utilisateurs, des applications utilisant l'API Kubernetes et du plan de contrôle. La journalisation d'audit est un composant de tous les clusters Kubernetes.

Pour plus d'informations, consultez la section [Audit](#) dans la documentation Kubernetes.

Amazon EKS permet aux journaux d'audit EKS d'être ingérés en tant qu'Amazon CloudWatch Logs via la fonction de [journalisation du plan de contrôle EKS](#). GuardDuty ne gère pas la journalisation de votre plan de contrôle Amazon EKS et ne rend pas les journaux d'audit EKS accessibles sur votre compte si vous ne les avez pas activés pour Amazon EKS. Pour gérer l'accès à vos journaux d'audit EKS et leur conservation, vous devez configurer la fonction de journalisation du plan de contrôle Amazon EKS. Pour de plus amples informations, veuillez consulter [Activation et désactivation de journaux de plan de contrôle](#) dans le Guide de l'utilisateur Amazon EKS.

Activation de la protection EKS dans les environnements à comptes multiples

Dans un environnement à comptes multiples, seul le compte d' GuardDuty administrateur délégué a la possibilité d'activer ou de désactiver la fonctionnalité EKS Protection ; pour les comptes des membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration depuis leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Ce compte d' GuardDuty administrateur délégué peut choisir d'activer automatiquement la protection EKS pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements à comptes multiples, consultez [Gérer plusieurs comptes sur Amazon](#). GuardDuty

Configuration de la surveillance du journal d'audit EKS pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour configurer la surveillance du journal d'audit EKS pour le compte GuardDuty d'administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Sous EKS Audit Logs, vous pouvez consulter l'état de configuration actuel de EKS Audit Log Monitoring.
4. Effectuez l'une des actions suivantes :

Utilisation d'Activer pour tous les comptes

- Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
- Choisissez Enregistrer.

Utilisation de Configurer les comptes manuellement

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.

- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Choisissez Enregistrer.

API/CLI

Exécutez l'opération d'API [updateDetector](#) en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features name` en tant que `EKS_AUDIT_LOGS` et `status` en tant que `ENABLED` ou `DISABLED`.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

Vous pouvez activer ou désactiver la surveillance du journal d'audit EKS en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser un compte GuardDuty d'administrateur délégué valide *detector ID*.

Note

L'exemple de code suivant active la surveillance des journaux d'audit EKS. Assurez-vous de *12abc34d567e8fa901bc2d34e56789f0* remplacer par le compte `detector-id` d' GuardDuty administrateur délégué et *55555555555* par le compte Compte AWS d' GuardDuty administrateur délégué.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Pour désactiver la surveillance des journaux d'audit EKS, remplacez `ENABLED` par `DISABLED`.

Auto-enable Surveillance du journal d'audit EKS pour tous les comptes des membres

Choisissez votre méthode d'accès préférée afin d'activer la surveillance des journaux d'audit EKS pour les comptes membres existants de votre organisation.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

Utilisation de la page Plans de protection

1. Dans le volet de navigation, sélectionnez Plans de protection.
2. Choisissez Configurer toutes les activations. Sous EKS Audit Logs, vous pouvez consulter l'état actuel de la surveillance des journaux d'audit EKS pour les comptes membres actifs de votre organisation.
3. Choisissez Activer pour tous les comptes. Cette action active automatiquement la surveillance des journaux d'audit EKS pour les comptes existants et nouveaux de l'organisation.
4. Choisissez Enregistrer tout, puis cliquez sur Confirmer et enregistrez.

Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez Auto-enable les préférences avant Ajouter des comptes sur invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous Surveillance des journaux d'audit EKS.
4. Choisissez Enregistrer.

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes et que vous souhaitez personnaliser la configuration de la surveillance des journaux d'audit EKS pour des comptes

spécifiques de votre organisation, veuillez consulter [Activer ou désactiver de manière sélective la surveillance des journaux d'audit EKS pour les comptes membres](#).

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance du journal d'audit EKS pour vos comptes membres, exécutez l'opération d'[updateMemberDetectors](#) API en utilisant la votre *detector ID*.
- L'exemple suivant montre comment activer la surveillance des journaux d'audit EKS pour un compte membre unique. Pour la désactiver, remplacez ENABLED par DISABLED.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```



Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer la surveillance des journaux d'audit EKS pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée afin d'activer la surveillance des journaux d'audit EKS pour tous les comptes membres actifs existants de votre organisation.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Sous EKS Audit Logs, dans la section Comptes membres actifs, sélectionnez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Enregistrer.

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance du journal d'audit EKS pour vos comptes membres, exécutez l'opération d'[updateMemberDetectors](#) API en utilisant la votre *detector ID*.
- L'exemple suivant montre comment activer la surveillance des journaux d'audit EKS pour un compte membre unique. Pour la désactiver, remplacez ENABLED par DISABLED.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Auto-enable Surveillance du journal d'audit EKS pour les nouveaux comptes de membres

Les comptes de membres nouvellement ajoutés doivent être activés GuardDuty avant de sélectionner la configuration de l'analyse des GuardDuty-initiated logiciels malveillants. Les comptes membres gérés par invitation peuvent configurer manuellement le scan des GuardDuty-initiated logiciels malveillants pour leurs comptes. Pour de plus amples informations, veuillez consulter [Step 3 - Accept an invitation](#).

Choisissez votre méthode d'accès préférée afin d'activer la surveillance des journaux d'audit EKS pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte GuardDuty administrateur délégué peut activer la surveillance du journal d'audit EKS pour les nouveaux comptes membres d'une organisation, à l'aide de la page EKS Audit Log Monitoring ou des comptes.

Pour activer automatiquement la surveillance des journaux d'audit EKS pour les nouveaux comptes membres

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

- À l'aide de la page Plans de protection :

1. Dans le volet de navigation, sélectionnez Plans de protection.
2. Choisissez Configurer toutes les activations. Sous EKS Audit Logs, configurez le paramètre d'activation automatique.
3. Choisissez Configurer les comptes manuellement.
4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la surveillance des journaux d'audit EKS sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
5. Choisissez Enregistrer.

- Utilisation de la page Comptes :
 1. Dans le panneau de navigation, choisissez Accounts (Comptes).
 2. Sur la page Comptes, sélectionnez Auto-enablePréférences.
 3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous Surveillance des journaux d'audit EKS.
 4. Choisissez Enregistrer.

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance du journal d'audit EKS pour vos nouveaux comptes, exécutez l'opération [UpdateOrganizationConfiguration](#) d'API en utilisant votre propre compte *detector ID*.
- L'exemple suivant montre comment activer la surveillance des journaux d'audit EKS pour les nouveaux membres qui rejoignent votre organisation. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Activer ou désactiver de manière sélective la surveillance des journaux d'audit EKS pour les comptes membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance des journaux d'audit EKS pour certains comptes membres de votre organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

Sur la page Comptes, veuillez consulter la colonne Surveillance des journaux d'audit EKS pour connaître l'état de votre compte membre.

3. Pour activer ou désactiver la surveillance des journaux d'audit EKS

Sélectionnez le compte que vous souhaitez configurer pour la surveillance des journaux d'audit EKS. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, choisissez Surveillance des journaux d'audit EKS, puis choisissez l'option appropriée.

API/CLI

Pour activer ou désactiver de manière sélective la surveillance du journal d'audit EKS pour vos comptes membres, appelez l'opération d'[updateMemberDetectors](#) API en utilisant la votre *detector ID*.

L'exemple suivant montre comment activer la surveillance des journaux d'audit EKS pour un compte membre unique. Pour la désactiver, remplacez ENABLED par DISABLED. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
"ENABLED"}]'
```

Activation de la protection EKS pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection sur son AWS compte dans une région spécifique.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations d'une invitation ou par le biais d'une invitation, cette section ne s'applique pas à vous. Pour plus d'informations sur la gestion de plusieurs comptes, consultez [Activation de la protection EKS dans les environnements à comptes multiples](#).

Après avoir activé la protection EKS, vous GuardDuty commencerez à surveiller les journaux d'audit EKS pour les clusters Amazon EKS de votre compte.

Choisissez votre méthode d'accès préférée pour activer la protection EKS dans votre compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le sélecteur de région situé dans le coin supérieur droit, sélectionnez la région dans laquelle vous souhaitez activer la protection EKS.
3. Dans le volet de navigation, sélectionnez Plans de protection.
4. Choisissez Configurer toutes les activations. Sous EKS Audit Logs, choisissez Activer pour activer la protection EKS.
5. Choisissez Enregistrer tout, puis cliquez sur Confirmer et enregistrez.

API/CLI

- Exécutez l'opération d'[updateDetector](#) API en utilisant l'ID de détecteur régional du compte GuardDuty administrateur délégué et en transmettant le nom de l'featuresobjet EKS_AUDIT_LOGS et le statut commeENABLED.

Vous pouvez également activer EKS Protection en exécutant la AWS CLI commande a. Exécutez la commande suivante et remplacez-la *12abc34d567e8fa901bc2d34e56789f0* par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection EKS.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]
```

GuardDuty Protection S3

Note

Vous pouvez configurer S3 Protection ainsi que tous les autres plans de protection à partir d'une seule page de la GuardDuty console. Pour de plus amples informations, veuillez consulter [Configuration des plans de protection](#).

S3 Protection vous aide à détecter les risques de sécurité potentiels liés aux données, tels que l'exfiltration et la destruction de données, dans vos compartiments Amazon Simple Storage Service (Amazon S3). GuardDuty surveille les événements liés aux AWS CloudTrail données pour Amazon S3, notamment les opérations d'API au niveau des objets afin d'identifier ces risques dans tous les compartiments Amazon S3 de votre compte.

Lorsqu'une menace potentielle est GuardDuty détectée sur la base de la surveillance des événements liés aux données S3, elle génère un constat de sécurité. Pour plus d'informations sur les types de recherche GuardDuty susceptibles d'être générés lorsque vous activez S3 Protection, consultez [GuardDuty Types de détection de la protection S3](#).

Par défaut, la détection des menaces de base inclut une surveillance [AWS CloudTrail événements de gestion](#) visant à identifier les menaces potentielles dans vos ressources Amazon S3. Cette source de données est différente des événements de AWS CloudTrail données pour S3 car elles surveillent toutes deux différents types d'activités dans votre environnement.

Vous pouvez activer S3 Protection dans un compte dans toutes les régions où [cette fonctionnalité est prise GuardDuty en charge](#). Cela vous aidera à surveiller les événements de CloudTrail données pour S3 dans ce compte et cette région. Une fois que vous GuardDuty aurez activé S3 Protection, vous serez en mesure de surveiller entièrement vos compartiments Amazon S3 et de détecter tout accès suspect aux données stockées dans vos compartiments S3.

Pour utiliser S3 Protection, il n'est pas nécessaire d'activer ou de configurer explicitement la connexion aux événements de données S3 AWS CloudTrail.

essai gratuit de 30 jours

La liste suivante explique comment l'essai gratuit de 30 jours fonctionnerait pour votre compte :

- Lorsque vous l'activez GuardDuty Compte AWS dans une nouvelle région pour la première fois, vous bénéficiez d'un essai gratuit de 30 jours. Dans ce cas, GuardDuty vous activez également S3 Protection, qui est incluse dans l'essai gratuit.
- Lorsque vous utilisez GuardDuty et décidez d'activer S3 Protection pour la première fois, votre compte dans cette région bénéficiera d'un essai gratuit de 30 jours pour S3 Protection.
- Vous pouvez choisir de désactiver la protection S3 dans n'importe quelle région à tout moment.
- Au cours de l'essai gratuit de 30 jours, vous pouvez obtenir une estimation de vos coûts d'utilisation pour ce compte et cette région. Après la fin de l'essai gratuit de 30 jours, S3 Protection n'est pas automatiquement désactivée. Votre compte dans cette région commencera à entraîner des frais d'utilisation. Pour de plus amples informations, veuillez consulter [Surveillance de GuardDuty l'utilisation et estimation des coûts](#).

AWS CloudTrail événements de données pour S3

Les événements de données, également appelés opérations de plan de données, fournissent des informations sur les opérations de ressource exécutées sur ou dans une ressource. Ils s'agit souvent d'activités dont le volume est élevé.

Voici des exemples d'événements de CloudTrail données GuardDuty pouvant être surveillés pour S3 :

- Opérations d'API `GetObject`
- Opérations d'API `PutObject`
- Opérations d'API `ListObjects`
- Opérations d'API `DeleteObject`

Pour plus d'informations sur ces API, consultez le manuel [Amazon Simple Storage Service API Reference](#).

Comment GuardDuty utilise les événements de CloudTrail données pour S3

Lorsque vous activez S3 Protection, GuardDuty commence à analyser les événements de CloudTrail données pour S3 provenant de tous vos compartiments S3 et à les surveiller pour détecter toute activité malveillante et suspecte. Pour de plus amples informations, veuillez consulter [AWS CloudTrail événements de gestion](#).

Lorsqu'un utilisateur non authentifié accède à un objet S3, cela signifie que celui-ci est accessible au public. Par conséquent, GuardDuty ne traite pas de telles demandes. GuardDuty traite les demandes adressées aux objets S3 en utilisant des informations d'identification IAM (Gestion des identités et des accès AWS) ou AWS STS (AWS Security Token Service) valides.

 Remarque

Après avoir activé S3 Protection, GuardDuty surveille les événements de données provenant des compartiments Amazon S3 résidant dans la même région que celle où vous l'avez activée GuardDuty.

Si vous désactivez la protection S3 sur votre compte dans une région spécifique, la surveillance des événements liés aux données stockées dans vos compartiments S3 est GuardDuty interrompue par S3. GuardDuty ne générera plus de types de recherche S3 Protection pour votre compte dans cette région.

GuardDuty utilisation d'événements de CloudTrail données pour S3 pour les séquences d'attaque

[GuardDuty Détection étendue des menaces](#) détecte les séquences d'attaque en plusieurs étapes qui couvrent les sources de données, les AWS ressources et la chronologie de base d'un compte. Lorsque GuardDuty vous observez une séquence d'événements indiquant une activité suspecte récente ou en cours sur votre compte, il GuardDuty génère une recherche de séquence d'attaque associée.

Par défaut, lorsque vous l'activez GuardDuty, la détection étendue des menaces est également activée dans votre compte. Cette fonctionnalité couvre le scénario de menace associé aux événements CloudTrail de gestion sans frais supplémentaires. Toutefois, pour utiliser pleinement le potentiel de la détection étendue des menaces, il est GuardDuty recommandé d'activer S3 Protection afin de couvrir les scénarios de menace associés aux événements de CloudTrail données pour S3.

Une fois que vous avez activé S3 Protection, GuardDuty elle couvre automatiquement les scénarios de menace liés à la séquence d'attaque, tels que la compromission ou la destruction de données, dans lesquels vos ressources Amazon S3 pourraient être impliquées.

Activation de la protection S3 dans les environnements à comptes multiples

Dans un environnement multi-comptes, seul le compte d' GuardDuty administrateur délégué a la possibilité de configurer (activer ou désactiver) S3 Protection pour les comptes des membres de son AWS organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration depuis leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Le compte d' GuardDuty administrateur délégué peut choisir d'activer automatiquement S3 Protection sur tous les comptes, uniquement sur les nouveaux comptes ou sur aucun compte de l'organisation. Pour de plus amples informations, veuillez consulter [Gestion de comptes avec AWS Organizations](#).

Activation de la protection S3 pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour activer S3 Protection pour le compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Protection S3.
3. Sur la page Protection S3, choisissez Modifier.
4. Effectuez l'une des actions suivantes :

Utilisation d'Activer pour tous les comptes

- Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
- Choisissez Enregistrer.

Utilisation de Configurer les comptes manuellement

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Choisissez Enregistrer.

API/CLI

[updateDetector](#) Exécuté en utilisant l'ID du détecteur du compte GuardDuty administrateur délégué pour la région en cours et en transmettant l'featuresobjet name sous S3_DATA_EVENTS et en status tant queENABLED.

Vous pouvez également configurer S3 Protection en utilisant AWS Command Line Interface. Exécutez la commande suivante et assurez-vous de le **12abc34d567e8fa901bc2d34e56789f0** remplacer par l'ID du détecteur du compte GuardDuty administrateur délégué pour la région actuelle.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Auto-enable Protection S3 pour tous les comptes membres de l'organisation

Choisissez votre méthode d'accès préférée pour activer S3 Protection pour le compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide de votre compte administrateur.

2. Effectuez l'une des actions suivantes :

Utilisation de la page Protection S3

1. Dans le panneau de navigation, choisissez Protection S3.
2. Choisissez Activer pour tous les comptes. Cette action active automatiquement la protection S3 pour les comptes existants et nouveaux de l'organisation.
3. Choisissez Enregistrer.

 Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez Auto-enable les préférences avant Ajouter des comptes sur invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous Protection S3.
4. Choisissez Enregistrer.

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter [Activer S3 Protection de manière sélective dans les comptes des membres](#).

API/CLI

- Pour activer S3 Protection de manière sélective pour vos comptes membres, appelez l'opération [updateMemberDetectors](#) d'API en utilisant la votre *detector ID*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Assurez-vous de remplacer *12abc34d567e8fa901bc2d34e56789f0* par le compte detector-id d' GuardDuty administrateur délégué, et *111122223333*.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

 Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer la protection S3 pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la protection S3 pour tous les comptes membres actifs existants de votre organisation.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Protection S3.
3. Sur la page Protection S3, vous pouvez afficher l'état actuel de la configuration. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Confirmer.

API/CLI

- Pour activer S3 Protection de manière sélective pour vos comptes membres, appelez l'opération [updateMemberDetectors](#) d'API en utilisant la votre *detector ID*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Assurez-vous de remplacer `12abc34d567e8fa901bc2d34e56789f0` par le compte `detector-id` d' GuardDuty administrateur délégué, et `111122223333`.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

 Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Auto-enable Protection S3 pour les nouveaux comptes de membres

Choisissez votre méthode d'accès préférée pour activer la protection S3 pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte d' GuardDuty administrateur délégué peut activer de nouveaux comptes membres dans une organisation via la console, en utilisant la page S3 Protection ou Comptes.

Pour activer automatiquement la protection S3 pour les nouveaux comptes membres

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

- Utilisation de la page Protection S3 :

1. Dans le panneau de navigation, choisissez Protection S3.
2. Sur la page Protection S3, choisissez Modifier.
3. Choisissez Configurer les comptes manuellement.

4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la protection S3 sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
 5. Choisissez Enregistrer.
- Utilisation de la page Comptes :
 1. Dans le panneau de navigation, choisissez Accounts (Comptes).
 2. Sur la page Comptes, sélectionnez Auto-enablePréférences.
 3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous Protection S3.
 4. Choisissez Enregistrer.

API/CLI

- Pour activer S3 Protection de manière sélective pour vos comptes membres, appelez l'opération [UpdateOrganizationConfiguration](#)d'API en utilisant la vôtre *detector ID*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Définissez les préférences pour activer ou désactiver automatiquement le plan de protection dans cette région pour les nouveaux comptes (NEW) qui rejoignent l'organisation, pour tous les comptes (ALL) ou pour aucun des comptes (NONE) de l'organisation. Pour plus d'informations, voir [auto EnableOrganizationMembers](#). Selon vos préférences, vous devrez peut-être remplacer NEW par ALL ou NONE.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer S3 Protection de manière sélective dans les comptes des membres

Choisissez votre méthode d'accès préférée pour activer S3 Protection de manière sélective pour les comptes des membres.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

Sur la page Comptes, veuillez consulter la colonne Protection S3 pour connaître l'état de votre compte membre.

3. Pour activer S3 Protection de manière sélective

Sélectionnez le compte pour lequel vous souhaitez activer S3 Protection. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, choisissez S3Pro, puis choisissez l'option appropriée.

API/CLI

Pour activer S3 Protection de manière sélective pour vos comptes membres, exécutez l'opération [updateMemberDetectors](#) API à l'aide de votre propre identifiant de détecteur. L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Pour la désactiver, remplacez `true` par `false`.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

 Note

Si vous utilisez des scripts pour intégrer de nouveaux comptes et que vous souhaitez désactiver la protection S3 dans vos nouveaux comptes, vous pouvez modifier l'opération d'API [createDetector](#) avec l'objet facultatif `dataSources`, comme décrit dans cette rubrique.

Activation de S3 Protection pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations d'une invitation ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour de plus amples informations, veuillez consulter [Activation de la protection S3 dans les environnements à comptes multiples](#).

Une fois que vous aurez activé S3 Protection, vous GuardDuty commencerez à surveiller les événements liés aux AWS CloudTrail données pour les compartiments S3 de votre compte.

Choisissez votre méthode d'accès préférée pour configurer la protection S3 pour un compte autonome.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le sélecteur de région situé dans le coin supérieur droit, sélectionnez la région dans laquelle vous souhaitez activer S3 Protection.
3. Dans le panneau de navigation, choisissez Protection S3.
4. La page Protection S3 fournit l'état actuel de la protection S3 pour votre compte. Choisissez Activer ou Désactiver pour activer ou désactiver la protection S3 à tout moment.
5. Choisissez Confirmer pour confirmer votre sélection.

API/CLI

Exécutez en [updateDetector](#) utilisant votre identifiant de détecteur valide pour la région actuelle et en transmettant l'featuresobjet name tel que S3_DATA_EVENTS défini ENABLED pour activer la protection S3, respectivement.

Note

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

Vous pouvez également utiliser AWS Command Line Interface. Pour activer S3 Protection, exécutez la commande suivante et remplacez-la *12abc34d567e8fa901bc2d34e56789f0* par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer S3 Protection.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

GuardDuty Surveillance du temps d'exécution

Note

Vous pouvez configurer le Runtime Monitoring ainsi que tous les autres plans de protection à partir d'une seule page de la GuardDuty console. Pour plus d'informations, consultez [Configuration des plans de protection](#).

Runtime Monitoring observe et analyse les événements au niveau du système d'exploitation, du réseau et des fichiers pour vous aider à détecter les menaces potentielles dans des AWS charges de travail spécifiques de votre environnement.

AWS Ressources prises en charge dans le domaine de la surveillance des temps d'exécution — Runtime Monitoring fournit une couverture de détection des menaces pour les ressources Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS AWS Fargate) on et Amazon Elastic Compute Cloud (Amazon EC2).

GuardDuty ne prend pas en charge les clusters Amazon EKS exécutés sur AWS Fargate.

Dans ce document et dans d'autres sections relatives à la surveillance du temps d'exécution, GuardDuty utilise la terminologie du type de ressource pour faire référence aux ressources Amazon EKS, Fargate, Amazon ECS et Amazon EC2.

La surveillance du temps d'exécution utilise un agent de GuardDuty sécurité qui ajoute de la visibilité sur le comportement d'exécution, comme l'accès aux fichiers, l'exécution des processus, les arguments de ligne de commande et les connexions réseau. Pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces potentielles, vous pouvez gérer l'agent de sécurité pour ce type de ressource spécifiquement automatiquement ou manuellement (à l'exception de Fargate (Amazon ECS uniquement)). La gestion automatique de l'agent de sécurité signifie que vous autorisez GuardDuty l'installation et la mise à jour de l'agent de sécurité en votre nom. D'autre part, lorsque vous gérez manuellement l'agent de sécurité pour vos ressources, vous êtes responsable de l'installer et de le mettre à jour, selon les besoins.

Cette fonctionnalité étendue GuardDuty peut vous aider à identifier et à répondre aux menaces potentielles susceptibles de cibler les applications et les données exécutées dans vos charges de travail et instances individuelles. Par exemple, une menace peut potentiellement commencer par compromettre un seul conteneur qui exécute une application web vulnérable. Cette application Web

peut disposer d'autorisations d'accès aux conteneurs et charges de travail sous-jacents. Dans ce scénario, des identifiants mal configurés pourraient potentiellement conduire à un accès plus large au compte et aux données qui y sont stockées.

En analysant les événements d'exécution des conteneurs et des charges de travail individuels, GuardDuty vous pouvez identifier la compromission d'un conteneur et des AWS informations d'identification associées dans une phase initiale, et détecter les tentatives d'augmentation des privilèges, les demandes d'API suspectes et les accès malveillants aux données de votre environnement.

Table des matières

- [Comment ça marche](#)
- [Comment fonctionne l'essai gratuit de 30 jours dans Runtime Monitoring](#)
- [Prérequis pour activer la surveillance d'exécution](#)
- [Activer la surveillance du GuardDuty temps d'exécution](#)
- [Gestion des agents GuardDuty de sécurité](#)
- [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#)
- [Configuration de la surveillance du processeur et de la mémoire](#)
- [Utilisation d'un VPC partagé avec surveillance du temps d'exécution](#)
- [Utilisation de l'infrastructure en tant que code \(IaC\) avec des agents de sécurité GuardDuty automatisés](#)
- [Types d'événements d'exécution collectés qui GuardDuty utilisent](#)
- [Agent d'hébergement GuardDuty de référentiels Amazon ECR](#)
- [Deux agents de sécurité sur le même hôte sous-jacent](#)
- [Surveillance du temps d'exécution EKS dans GuardDuty](#)
- [GuardDuty versions publiées de l'agent de sécurité](#)
- [Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring](#)

Comment ça marche

La surveillance du temps d'exécution utilise un agent de sécurité léger pour observer le comportement d'exécution de vos charges de travail Amazon EC2, Amazon EKS et Amazon ECS sur Fargate et détecter les menaces. Cela fonctionne de bout en bout comme suit :

1. L'agent est déployé sur vos ressources. GuardDuty vous pouvez déployer et mettre à jour l'agent pour vous (configuration automatique de l'agent), ou vous pouvez le déployer et le gérer vous-même (configuration manuelle de l'agent). Les étapes dépendent du type de ressource.
2. L'agent collecte les événements d'exécution. Sur chaque ressource surveillée, l'agent observe l'activité au niveau du système d'exploitation, telle que l'exécution des processus, l'accès aux fichiers et les connexions réseau.
3. L'agent envoie des événements à GuardDuty. L'agent transmet les événements au GuardDuty backend. Les données restent sur le AWS réseau et les événements transmis à partir de vos ressources informatiques GuardDuty ne sont pas facturés GuardDuty. Pour plus de détails, consultez [Comment l'agent de sécurité se connecte à GuardDuty](#).
4. GuardDuty analyse les événements et génère des conclusions. Lorsqu'il détecte un comportement suspect, tel qu'une augmentation de privilèges ou une communication avec un hôte malveillant connu, il GuardDuty génère une constatation. Pour consulter la liste actualisée des résultats GuardDuty générés, voir [GuardDuty Types de recherche liés à la surveillance du temps](#).

L'agent fonctionne dans les limites de processeur et de mémoire définies, de sorte que sa consommation de ressources reste prévisible et ne dégrade pas les performances ou la disponibilité des charges de travail exécutées sur le même hôte. Pour connaître ces limites, voir [Prérequis pour activer la surveillance d'exécution](#).

Table des matières

- [Activer la surveillance du temps d'exécution](#)
- [Déploiement de l'agent de sécurité sur Amazon EKS](#)
- [Déploiement de l'agent de sécurité sur Amazon EC2](#)
- [Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate](#)
- [Comment l'agent de sécurité se connecte à GuardDuty](#)
- [Suivi du temps d'exécution Surveillance de la couverture](#)

Activer la surveillance du temps d'exécution

L'activation de la surveillance du temps d'exécution s'effectue en deux étapes :

1. Activez la surveillance du temps d'exécution pour votre compte. GuardDuty accepte ensuite les événements d'exécution provenant de vos instances Amazon EC2, de vos clusters Amazon ECS et de vos charges de travail Amazon EKS.

2. Gérez l'agent GuardDuty de sécurité pour les ressources que vous souhaitez surveiller. En fonction du type de ressource, vous pouvez :

- Utiliser la configuration automatisée de l'agent : GuardDuty déploie l'agent et établit sa connectivité.
- Gérez l'agent manuellement : vous créez un point de terminaison VPC et vous gérez l'installation et les mises à jour de l'agent.

La gestion de l'agent varie selon le type de ressource. Pour plus d'informations, voir :

- [Déploiement de l'agent de sécurité sur Amazon EKS](#)
- [Déploiement de l'agent de sécurité sur Amazon EC2](#)
- [Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate](#)

Lorsque l'agent GuardDuty de sécurité est déployé sur une instance Amazon EC2 et reçoit des événements d'exécution de celle-ci, il GuardDuty ne vous facture pas l'analyse des journaux Compte AWS de flux VPC provenant de cette instance. Cela permet d'éviter le double coût d'utilisation.

Déploiement de l'agent de sécurité sur Amazon EKS

GuardDuty La surveillance du temps d'exécution surveille vos clusters Amazon EKS pour détecter les menaces en y déployant l'agent de GuardDuty sécurité. Sur Amazon EKS, GuardDuty déploie l'agent en tant que [module complémentaire aws-guardduty-agent EKS](#).

Remarques

La surveillance du temps d'exécution prend en charge les clusters Amazon EKS exécutés sur des instances Amazon EC2 et le mode automatique Amazon EKS.

La surveillance du temps d'exécution ne prend pas en charge les clusters Amazon EKS dotés de nœuds hybrides Amazon EKS, ni ceux qui s'exécutent sur AWS Fargate.

Pour plus d'informations sur ces fonctionnalités d'Amazon EKS, consultez [Qu'est-ce qu'Amazon EKS ?](#) dans le guide de l'utilisateur Amazon EKS.

Vous pouvez laisser GuardDuty gérer l'agent automatiquement (recommandé) ou le gérer manuellement.

Configuration automatique de l'agent (recommandée)

GuardDuty gère le déploiement et les mises à jour de l'agent de sécurité pour vos clusters EKS. Dans la GuardDuty console, cette configuration apparaît sous le nom de Runtime Monitoring (EKS).

Pour savoir comment l'agent de sécurité se connecte à GuardDuty, voir [Comment l'agent de sécurité se connecte à GuardDuty](#).

Impact de l'activation de l'agent de sécurité

GuardDuty déploie l'agent de sécurité sur vos clusters EKS, et Amazon Elastic Kubernetes Service (Amazon EKS) coordonne son déploiement sur les nœuds.

Périmètre de surveillance

Par défaut, GuardDuty gère l'agent de sécurité pour tous les clusters EKS de votre compte, y compris les nouveaux clusters que vous créez. Pour arrêter GuardDuty de gérer l'agent sur un cluster spécifique, ajoutez le tag `GuardDutyManaged : false` à ce cluster.

Pour plus d'informations sur le balisage des clusters EKS, consultez la section [Marquage de vos ressources Amazon EKS](#) dans le guide de l'utilisateur Amazon EKS.

Considérations

- Lorsque la configuration automatique de l'agent est désactivée, GuardDuty gère l'agent de sécurité uniquement sur les clusters EKS auxquels vous ajoutez `GuardDutyManaged : true`.
- L'ajout de la `false` balise `GuardDutyManaged` : arrête la gestion GuardDuty de l'agent de sécurité, mais ne désinstalle pas un agent déjà installé.
- Protégez le `GuardDutyManaged` tag en contrôlant qui peut le modifier, à l'aide de politiques de contrôle des services ou de politiques IAM. Pour plus d'informations, veuillez consulter [Politiques de contrôle des services \(SCP\)](#) dans le Guide de l'utilisateur AWS Organizations ou le [Contrôle de l'accès aux ressources AWS](#) dans le Guide de l'utilisateur IAM.

Configuration manuelle de l'agent

Utilisez cette approche lorsque vous souhaitez déployer et gérer manuellement l'agent GuardDuty de sécurité sur tous vos clusters EKS. Assurez-vous que la surveillance du temps d'exécution est activée pour vos comptes. L'agent GuardDuty de sécurité risque de ne pas fonctionner comme prévu si la surveillance du temps d'exécution n'est pas activée.

Impact de l'utilisation de cette approche

Vous devez coordonner le déploiement de l'agent GuardDuty de sécurité au sein de vos clusters EKS sur tous vos comptes. Pour bénéficier des dernières fonctionnalités de sécurité, vous devez également mettre à jour l'agent lors de la GuardDuty publication d'une nouvelle version. Pour plus d'informations sur les versions des agents pour EKS, consultez [GuardDuty versions de l'agent de sécurité pour les ressources Amazon EKS](#).

Considérations

Vous devez garantir un flux de données sécurisé tout en surveillant et en comblant les lacunes de couverture à mesure que de nouveaux clusters et de nouvelles charges de travail sont déployés en permanence.

Rubriques associées

- [Comment l'agent de sécurité se connecte à GuardDuty](#)
- [Suivi du temps d'exécution Surveillance de la couverture](#)

Déploiement de l'agent de sécurité sur Amazon EC2

GuardDuty Runtime Monitoring surveille vos instances Amazon EC2 pour détecter les menaces en y déployant l'agent GuardDuty de sécurité.

Note

Runtime Monitoring collecte également les événements d'exécution issus des tâches Amazon ECS exécutées sur vos instances Amazon EC2.

Vous pouvez laisser GuardDuty gérer l'agent automatiquement (recommandé) ou le gérer manuellement.

Configuration automatique de l'agent (recommandée)

GuardDuty gère le déploiement et les mises à jour de l'agent de sécurité pour vos instances Amazon EC2. Dans la GuardDuty console, cette configuration apparaît sous le nom Runtime Monitoring (EC2).

Pour savoir comment l'agent de sécurité se connecte à GuardDuty, voir [Comment l'agent de sécurité se connecte à GuardDuty](#).

Impact de l'activation de l'agent de sécurité

Avec la configuration automatique de l'agent, GuardDuty crée une association SSM pour vos instances SSM-managed Amazon EC2 (illustrée sous Fleet Manager dans <https://console.aws.amazon.com/systems-manager/> la console) et l'utilise pour installer et mettre à jour l'agent.

Périmètre de surveillance

Par défaut, GuardDuty gère l'agent de sécurité pour toutes les instances Amazon EC2 de votre compte. Pour arrêter GuardDuty de gérer l'agent sur une instance spécifique, ajoutez le tag `GuardDutyManaged : false` à cette instance.

Considérations

- Lorsque la configuration automatique de l'agent est désactivée, GuardDuty gère l'agent de sécurité uniquement sur les instances Amazon EC2 que vous balisez avec `GuardDutyManaged : true`
- L'ajout de la `false` balise `GuardDutyManaged` : arrête la gestion GuardDuty de l'agent de sécurité, mais ne désinstalle pas un agent déjà installé.
- Protégez le `GuardDutyManaged` tag en contrôlant qui peut le modifier, à l'aide de politiques de contrôle des services ou de politiques IAM. Pour plus d'informations, veuillez consulter [Politiques de contrôle des services \(SCP\)](#) dans le Guide de l'utilisateur AWS Organizations ou le [Contrôle de l'accès aux ressources AWS](#) dans le Guide de l'utilisateur IAM.

Configuration manuelle de l'agent

Il existe deux méthodes pour gérer manuellement l'agent de sécurité pour Amazon EC2 :

- Pour les instances SSM-managed Amazon EC2, vous pouvez utiliser des documents GuardDuty gérés AWS Systems Manager pour installer l'agent de sécurité.

Note

Pour utiliser cette option, assurez-vous que chaque nouvelle instance Amazon EC2 que vous lancez est activée par SSM.

- Utilisez des scripts RPM Package Manager (RPM) pour installer l'agent de sécurité sur vos instances Amazon EC2, qu'elles soient ou non gérées par SSM.

Rubriques associées

- [Comment l'agent de sécurité se connecte à GuardDuty](#)
- [Suivi du temps d'exécution Surveillance de la couverture](#)

Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate

GuardDuty La surveillance du temps d'exécution surveille vos clusters Amazon ECS sur Fargate pour détecter les menaces en y déployant GuardDuty l'agent de sécurité.

Note

La surveillance du temps d'exécution ne prend pas en charge les applications exécutées sur les [instances gérées Amazon ECS](#).

GuardDuty gère automatiquement l'agent ; la gestion manuelle n'est pas disponible pour Fargate. Dans la GuardDuty console, cette configuration apparaît sous le nom de Runtime Monitoring (ECS).

Configuration automatique de l'agent (recommandée)

GuardDuty gère le déploiement et les mises à jour de l'agent de sécurité pour les nouvelles tâches Fargate dans vos clusters Amazon ECS.

Pour savoir comment l'agent de sécurité se connecte à GuardDuty, voir [Comment l'agent de sécurité se connecte à GuardDuty](#).

Impact de l'activation de l'agent de sécurité

Pour chaque nouvelle tâche Fargate GuardDuty , attache un conteneur annexe qui exécute l'agent de sécurité et collecte les événements d'exécution des conteneurs de la tâche.

L'image du sidecar est stockée dans Amazon Elastic Container Registry (Amazon ECR), avec des couches dans Amazon S3, et est extraite au démarrage de la tâche. Selon la configuration de votre réseau, vous devrez peut-être autoriser l'accès à ECR et à S3. Par exemple, autorisez la liste

de préfixes gérés S3 si vous utilisez des groupes de sécurité restreints. Pour plus d'informations, consultez [Conditions préalables à l'accès aux images du conteneur](#).

Si le sidecar ne peut pas démarrer, la surveillance du temps d'exécution n'empêche pas l'exécution de la tâche. Les tâches Fargate ne peuvent pas être modifiées une fois qu'elles ont commencé. Le sidecar GuardDuty est donc attaché au lancement de la tâche.

Périmètre de surveillance

Par défaut, GuardDuty gère l'agent de sécurité pour tous les clusters Amazon ECS de votre compte. Pour arrêter GuardDuty de gérer l'agent sur un cluster spécifique, ajoutez le tag `GuardDutyManaged : false` à ce cluster.

Pour plus d'informations sur la gestion de l'agent pour les tâches Fargate, consultez. [Gestion de l'agent de sécurité automatisé pour Fargate \(Amazon ECS uniquement\)](#)

Considérations

- Lorsque la configuration automatique de l'agent est désactivée, GuardDuty gère l'agent de sécurité uniquement sur les clusters Amazon ECS auxquels vous ajoutez `GuardDutyManaged : true`.
- L'ajout de la `false` balise `GuardDutyManaged` : arrête la gestion GuardDuty de l'agent de sécurité, mais ne désinstalle pas un agent déjà installé.
- Protégez le `GuardDutyManaged` tag en contrôlant qui peut le modifier, à l'aide de politiques de contrôle des services ou de politiques IAM. Pour plus d'informations, veuillez consulter [Politiques de contrôle des services \(SCP\)](#) dans le Guide de l'utilisateur AWS Organizations ou le [Contrôle de l'accès aux ressources AWS](#) dans le Guide de l'utilisateur IAM.

Rubriques associées

- [Comment l'agent de sécurité se connecte à GuardDuty](#)
- [Suivi du temps d'exécution Surveillance de la couverture](#)

Comment l'agent de sécurité se connecte à GuardDuty

L'agent de sécurité Runtime Monitoring fournit des événements d'exécution à GuardDuty. Les données restent sur le AWS réseau. Il n'y a aucun coût supplémentaire pour la connectivité GuardDuty configurée. Pour authentifier l'agent, GuardDuty utilise les [rôles d'identité de l'instance](#).

Pour Amazon ECS sur Fargate GuardDuty , utilisez le rôle d'exécution des tâches ; voir. [Conditions d'autorisation](#)

GuardDuty prend en charge deux méthodes de connectivité : link-local et point de terminaison Amazon VPC. L'agent de sécurité tente de se connecter à l'aide de ces méthodes pour transmettre des événements d'exécution à GuardDuty.

Grâce à la configuration automatique des agents, GuardDuty établit automatiquement la connectivité. Si vous gérez l'agent manuellement, vous devez créer un point de terminaison Amazon VPC.

Link-local connectivité

L'agent se connecte au GuardDuty backend via une adresse lien-local, à l'adresse. `guardduty-data-v2.us-east-1.amazonaws.com` Link-local la connectivité n'utilise pas de DNS privé. Le Région AWS (*us-east-1*) change en fonction de votre région.

Connectivité des points de terminaison Amazon VPC

L'agent se connecte au GuardDuty backend via un point de terminaison Amazon VPC. Il résout le nom DNS privé du point de terminaison et se connecte à celui-ci. Pour un point de terminaison non FIPS, c'est. `guardduty-data.us-east-1.amazonaws.com` Le Région AWS (*us-east-1*) change en fonction de votre région.

La ressource doit disposer d'un chemin réseau valide vers un point de terminaison `guardduty-data` Amazon VPC actif. GuardDuty sélectionne le sous-réseau en fonction de la disponibilité des adresses IP. Pour les topologies réseau avancées, vérifiez que la connectivité est possible.

Conditions préalables

Pour les prérequis, voir [Prérequis pour activer la surveillance d'exécution](#).

Considérations

- Tous les VPC — Grâce à la configuration automatique des agents, GuardDuty configurez la connectivité entre tous vos VPC, y compris les VPC centralisés et en étoile. Pour plus d'informations sur les VPC centralisés, consultez la section [Interface VPC](#) endpoints AWS du livre blanc intitulé « Création d'une infrastructure réseau évolutive et sécurisée ». Multi-VPC AWS
- VPC partagé : si vous utilisez un VPC partagé, utilisez GuardDuty ce VPC partagé pour recevoir les événements d'exécution de vos ressources une fois les conditions requises remplies. Consultez [Utilisation d'un VPC partagé avec surveillance du temps d'exécution](#).

Rubriques associées

- [Déploiement de l'agent de sécurité sur Amazon EC2](#)
- [Déploiement de l'agent de sécurité sur Amazon EKS](#)
- [Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate](#)
- [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#)

Suivi du temps d'exécution Surveillance de la couverture

Après avoir activé la surveillance du temps d'exécution et installé l'agent de GuardDuty sécurité sur votre compte autonome ou sur plusieurs comptes membres, vous pouvez suivre les étapes suivantes pour vous assurer que le paramètre du plan de protection fonctionne comme prévu et surveiller la quantité de mémoire et de processeur utilisée par l'agent GuardDuty de sécurité.

Évaluez la couverture d'exécution

GuardDuty vous recommande d'évaluer en permanence l'état de couverture de la ressource sur laquelle vous avez déployé l'agent de sécurité. L'état de couverture peut être sain ou malsain. Un état de couverture sain indique que la ressource correspondante GuardDuty reçoit les événements d'exécution en cas d'activité au niveau du système d'exploitation.

Lorsque l'état de couverture devient sain pour la ressource, elle GuardDuty est en mesure de recevoir les événements d'exécution et de les analyser pour détecter les menaces. Lorsque GuardDuty détecte une menace de sécurité potentielle dans les tâches ou les applications exécutées dans vos instances et charges de travail de conteneur, GuardDuty génère [GuardDuty Types de recherche liés à la surveillance du temps](#).

Vous pouvez également configurer un Amazon EventBridge (EventBridge) pour recevoir une notification lorsque le statut de couverture passe de Malsain à Santé ou autre. Pour plus d'informations, consultez [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#).

Configuration de la surveillance du processeur et de la mémoire pour l'agent GuardDuty de sécurité

Après avoir vérifié que l'état de couverture est « sain », vous pouvez évaluer les performances de l'agent de sécurité pour votre type de ressource. Pour les clusters Amazon EKS dotés de la version 1.5 ou supérieure de l'agent de sécurité, GuardDuty prend en charge la configuration des paramètres de l'agent de sécurité (module complémentaire). Pour plus d'informations, consultez [Configuration de la surveillance du processeur et de la mémoire](#).

Comment fonctionne l'essai gratuit de 30 jours dans Runtime Monitoring

La période d'essai gratuite de 30 jours fonctionne différemment pour les nouveaux GuardDuty comptes et pour les comptes existants qui ont déjà activé EKS Runtime Monitoring avant que la fonctionnalité de surveillance du temps d'exécution ne soit étendue aux instances Amazon EC2 et AWS Fargate (Amazon ECS uniquement).

J'utilise la période GuardDuty d'essai ou je n'ai jamais activé EKS Runtime Monitoring

La liste suivante explique comment fonctionne la période d'essai gratuite de 30 jours si vous utilisez la période d'essai de GuardDuty 30 jours ou si vous n'avez jamais activé EKS Runtime Monitoring :

- Lorsque vous l'activez GuardDuty pour la première fois, la surveillance du temps d'exécution et la surveillance du temps d'exécution EKS ne sont pas activées par défaut.

Lorsque vous activez la surveillance du temps d'exécution pour votre compte ou votre organisation, assurez-vous de configurer également l'agent de GuardDuty sécurité pour la ressource que vous souhaitez surveiller pour détecter les menaces. Par exemple, si vous souhaitez utiliser la surveillance du temps d'exécution pour vos instances Amazon EC2, vous devez également configurer l'agent de sécurité pour Amazon EC2 après l'avoir activé. Vous pouvez choisir de le faire manuellement ou automatiquement GuardDuty.

- Le plan de protection Runtime Monitoring est activé au niveau du compte. La période d'essai gratuite de 30 jours fonctionne au niveau des ressources. Une fois que l'agent de GuardDuty sécurité est déployé sur un type de ressource spécifique, l'essai gratuit de 30 jours commence lorsque le premier événement d'exécution associé à ce type de ressource est GuardDuty reçu. Par exemple, vous avez déployé l' GuardDutyagent au niveau des ressources (pour l'instance Amazon EC2, le cluster Amazon ECS et le cluster Amazon EKS). Dès GuardDuty réception du premier événement d'exécution pour une instance Amazon EC2, l'essai gratuit de 30 jours commence uniquement pour Amazon EC2.
- Lorsque vous souhaitez activer uniquement EKS Runtime Monitoring : lorsque vous l'activez GuardDuty pour la première fois, EKS Runtime Monitoring n'est pas activé par défaut (après la sortie de Runtime Monitoring). Vous devez activer EKS Runtime Monitoring. Pour l'utiliser de manière optimale, assurez-vous de gérer l'agent de GuardDuty sécurité manuellement ou d'activer la configuration automatique de l'agent afin qu'il GuardDuty gère l'agent en votre nom. Votre

période d'essai gratuite de 30 jours pour EKS Runtime Monitoring commence lorsque GuardDuty vous recevez son premier événement d'exécution pour la ressource Amazon EKS.

J'ai activé EKS Runtime Monitoring avant le lancement de Runtime Monitoring

Utilisez cette section uniquement lorsque la surveillance du temps d'exécution EKS a été activée pour vous Compte AWS et que vous souhaitez maintenant passer à la surveillance du temps d'exécution.

La liste suivante inclut des scénarios susceptibles de s'appliquer à votre cas d'utilisation de l'activation de la surveillance du temps d'exécution :

- Pour un GuardDuty compte existant sur lequel le plan de protection EKS Runtime Monitoring est activé et qui utilise l'expérience de GuardDuty console pour utiliser ce plan de protection : avec l'annonce de Runtime Monitoring, l'expérience de la console EKS Runtime Monitoring est désormais consolidée dans Runtime Monitoring. Votre configuration actuelle pour EKS Runtime Monitoring reste la même. Vous pouvez continuer à utiliser le API/CLI support pour effectuer des opérations associées à EKS Runtime Monitoring.
- Pour utiliser EKS Runtime Monitoring dans le cadre de Runtime Monitoring, vous devez configurer le Runtime Monitoring pour votre compte ou votre organisation. Pour conserver la même configuration pour la surveillance du temps d'exécution, voir [Migration de la surveillance d'exécution EKS vers la surveillance d'exécution](#). Toutefois, cela n'aura aucune incidence sur votre essai gratuit de 30 jours pour la ressource Amazon EKS.
- Le plan de protection Runtime Monitoring est activé au niveau du compte par région. Une fois l'agent de GuardDuty sécurité déployé sur l'un des types de ressources spécifiés (instance Amazon EC2 et cluster Amazon ECS), l'essai gratuit de 30 jours commence à la GuardDuty réception du premier événement d'exécution associé à la ressource. Un essai gratuit de 30 jours est associé à chaque type de ressource.

Par exemple, après avoir activé la surveillance du temps d'exécution, vous choisissez de déployer l' GuardDuty agent uniquement sur une instance Amazon EC2. L'essai gratuit de 30 jours pour cette ressource ne débutera que lors de la GuardDuty réception de son premier événement d'exécution pour une instance Amazon EC2. Plus tard, lorsque vous déploierez l' GuardDuty agent pour Fargate (Amazon ECS uniquement), l'essai gratuit de 30 jours pour cette ressource GuardDuty ne débutera que lors de la réception de son premier événement d'exécution pour le cluster Amazon ECS. Si vous avez déjà activé EKS Runtime Monitoring pour votre compte, GuardDuty cela ne réinitialise pas l'essai gratuit de 30 jours pour une ressource Amazon EKS.

Prérequis pour activer la surveillance d'exécution

Pour activer la surveillance du temps d'exécution et gérer l'agent de GuardDuty sécurité, vous devez remplir les conditions requises pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces. Chaque type de ressource comporte des prérequis différents. Par exemple, GuardDuty prend en charge différentes distributions du système d'exploitation en fonction du type de ressource.

Lorsque vous souhaitez surveiller uniquement les ressources Amazon EC2, vous devez respecter les conditions requises pour les instances Amazon EC2. Si, ultérieurement, vous choisissez de surveiller les ressources Amazon EKS, vous devez respecter les prérequis spécifiques aux clusters Amazon EKS.

Les sections suivantes incluent les prérequis en fonction du type de ressource.

Table des matières

- [Conditions préalables à la prise en charge des instances Amazon EC2](#)
- [Conditions préalables au support de ECS-EC2 Bottlerocket](#)
- [Prérequis pour AWS Fargate \(Amazon ECS uniquement\) support](#)
- [Conditions préalables à la prise en charge des clusters Amazon EKS](#)
- [Architectures de processeur, systèmes d'exploitation et versions de noyau pris en charge](#)

Conditions préalables à la prise en charge des instances Amazon EC2

Cette section inclut les conditions préalables à la surveillance du comportement d'exécution de vos instances Amazon EC2. Une fois ces conditions préalables remplies, voir [Activer la surveillance du GuardDuty temps d'exécution](#).

Rubriques

- [Gérer les instances EC2 par SSM \(pour la configuration automatique des agents uniquement\)](#)
- [Valider les exigences architecturales](#)
- [Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes](#)
- [Lors de l'utilisation de la configuration automatique des agents](#)
- [Limite du processeur et de la mémoire pour GuardDuty l'agent](#)
- [Étape suivante](#)

Gérer les instances EC2 par SSM (pour la configuration automatique des agents uniquement)

GuardDuty utilise AWS Systems Manager (SSM) pour déployer, installer et gérer automatiquement l'agent de sécurité sur vos instances. Si vous prévoyez d'installer et de gérer manuellement l'agent GuardDuty, le SSM n'est pas nécessaire.

Pour gérer vos instances Amazon EC2 avec Systems Manager, consultez la section [Configuration de Systems Manager pour les instances Amazon EC2](#) dans AWS Systems Manager le guide de l'utilisateur.

Valider les exigences architecturales

L'architecture de la distribution de votre système d'exploitation peut avoir un impact sur le comportement GuardDuty de l'agent de sécurité. Vous devez répondre aux exigences suivantes avant d'utiliser Runtime Monitoring pour les instances Amazon EC2 :

Pour les architectures de processeur, les distributions du système d'exploitation et les versions du noyau vérifiées, consultez [Architectures de processeur, systèmes d'exploitation et versions de noyau pris en charge](#).

- Exigences supplémentaires : uniquement si vous possédez Amazon ECS/Amazon EC2

Pour Amazon ECS/Amazon EC2, nous vous recommandons d'utiliser les dernières ECS-optimized AMI Amazon (datées du 29 septembre 2023 ou version ultérieure) ou d'utiliser la version v1.77.0 de l'agent Amazon ECS.

Affichage et mise à jour des valeurs **RLIMIT_MEMLOCK**

Lorsque la **RLIMIT_MEMLOCK** limite de votre système est trop faible, l'agent GuardDuty de sécurité risque de ne pas fonctionner comme prévu. GuardDuty recommande que les limites strictes et souples soient d'au moins 32 Mo. Si vous ne mettez pas à jour les limites, vous ne pouvez pas surveiller les événements d'exécution de votre ressource. Lorsque **RLIMIT_MEMLOCK** est supérieur aux limites minimales indiquées, il est facultatif pour vous de mettre à jour ces limites.

Vous pouvez modifier la **RLIMIT_MEMLOCK** valeur par défaut avant ou après l'installation de l'agent GuardDuty de sécurité.

Pour afficher les valeurs **RLIMIT_MEMLOCK**

1. Exécutez `ps aux | grep guardduty`. Cela produira l'ID du processus (pid).
2. Copiez l'ID du processus (pid) à partir de la sortie de la commande précédente.
3. Exécutez `grep "Max locked memory" /proc/pid/limits` après avoir pid remplacé le par l'ID de processus copié à l'étape précédente.

Cela affichera la quantité maximale de mémoire verrouillée pour exécuter l'agent GuardDuty de sécurité.

Pour mettre à jour les valeurs **RLIMIT_MEMLOCK**

1. Si le `/etc/systemd/system.conf.d/NUMBER-limits.conf` fichier existe, commentez la ligne `DefaultLimitMEMLOCK` de ce fichier. Ce fichier définit une valeur par défaut `RLIMIT_MEMLOCK` avec une priorité élevée, qui remplace vos paramètres dans le `/etc/systemd/system.conf` fichier.
2. Ouvrez le `/etc/systemd/system.conf` fichier et décommentez la ligne qui le contient `#DefaultLimitMEMLOCK=`.
3. Mettez à jour la valeur par défaut en fournissant des `RLIMIT_MEMLOCK` limites strictes et souples d'au moins 32 Mo. La mise à jour devrait ressembler à ceci `:DefaultLimitMEMLOCK=32M:32M`. Le format est `soft-limit:hard-limit`.
4. Exécutez `sudo reboot`.

Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes

Si vous avez défini une politique de contrôle des services (SCP) pour gérer les autorisations dans votre organisation, vérifiez que la limite des autorisations autorise `lguardduty:SendSecurityTelemetryaction`. GuardDuty nécessite cette autorisation pour prendre en charge la surveillance du temps d'exécution sur différents types de ressources.

Si votre compte est un compte membre, contactez l'administrateur délégué associé. Pour plus d'informations sur la gestion des SCP pour votre organisation, voir [Politiques de contrôle des services \(SCP\)](#).

Lors de l'utilisation de la configuration automatique des agents

Pour [Configuration automatique de l'agent \(recommandée\)](#) cela, vous Compte AWS devez remplir les prérequis suivants :

- Lorsque vous utilisez des balises d'inclusion avec une configuration d'agent automatisée, GuardDuty pour créer une association SSM pour une nouvelle instance, assurez-vous que la nouvelle instance est gérée par SSM et qu'elle apparaît sous Fleet Manager dans la <https://console.aws.amazon.com/systems-manager/console>.
- Lorsque vous utilisez des balises d'exclusion avec une configuration automatique de l'agent :
 - Ajoutez le `false` tag `GuardDutyManaged` : avant de configurer l'agent GuardDuty automatique pour votre compte.

Assurez-vous d'ajouter la balise d'exclusion à vos instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

- Activez le paramètre Autoriser les balises dans les métadonnées pour vos instances. Ce paramètre est obligatoire car il faut lire la balise d'exclusion du service de métadonnées d'instance (IMDS) pour déterminer s'il doit exclure l'instance de l'installation de l'agent. Pour plus d'informations, consultez [Activer l'accès aux balises dans les métadonnées des instances](#) dans le guide de l'utilisateur Amazon EC2.

Limite du processeur et de la mémoire pour GuardDuty l'agent

Limite du processeur

GuardDuty limite l'agent de sécurité à 10 % de la capacité totale du vCPU de l'instance. Par exemple, sur une instance dotée de 4 cœurs de vCPU, l'agent peut utiliser au maximum 0,4 vCPU.

Limite de mémoire

Parmi la mémoire associée à votre instance Amazon EC2, l'agent de GuardDuty sécurité peut utiliser une quantité limitée de mémoire.

Le tableau suivant indique la limite de mémoire.

Mémoire de l'instance Amazon EC2	Mémoire maximale pour l' GuardDuty agent
Moins de 8 Go	128 Mo
8 Go à moins de 32 Go	256 Mo
Plus ou égal à 32 Go	1 Go

Étape suivante

L'étape suivante consiste à configurer la surveillance du temps d'exécution et à gérer l'agent de sécurité (automatiquement ou manuellement).

Conditions préalables au support de ECS-EC2 Bottlerocket

Important

Cette section s'applique uniquement aux versions Bottlerocket ECS-optimized AMI v1.62.1 et supérieures, y compris les variantes suivantes :

- `bottlerocket-aws-ecs-2-x86_64 / bottlerocket-aws-ecs-2-aarch64`
- `bottlerocket-aws-ecs-3-x86_64 / bottlerocket-aws-ecs-3-aarch64`
- `bottlerocket-aws-ecs-2-nvidia / bottlerocket-aws-ecs-2-nvidia-fips`
- `bottlerocket-aws-ecs-3-nvidia / bottlerocket-aws-ecs-3-nvidia-fips`

Runtime Monitoring étend GuardDuty la détection des menaces à vos instances Bottlerocket Amazon EC2 dans les clusters Amazon ECS, en utilisant un agent de sécurité qui s'exécute en tant que conteneur hôte conformément à la conception optimisée de Bottlerocket pour les conteneurs. Pour l'activer, remplissez les conditions requises dans cette section. Une fois ces conditions préalables remplies, voir [Activer la surveillance du GuardDuty temps d'exécution](#).

Pour plus d'informations sur les exigences et les instructions, consultez [Gestion GuardDuty de l'agent de sécurité sur Bottlerocket \(Amazon ECS sur Amazon EC2\)](#).

Rubriques

- [Gérer les instances EC2 par SSM et configurer les autorisations des instances](#)

- [Validation des exigences architecturales](#)
- [Exigences en matière de connectivité réseau](#)
- [Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes](#)
- [Lors de l'utilisation de la configuration automatique des agents](#)
- [Limite du processeur et de la mémoire pour GuardDuty l'agent](#)
- [Étape suivante](#)

Gérer les instances EC2 par SSM et configurer les autorisations des instances

GuardDuty utilise AWS Systems Manager (SSM) pour déployer, installer et gérer l'agent de sécurité sur vos instances Bottlerocket, en passant par l'agent SSM dans le conteneur de contrôle Bottlerocket.

Dans la plupart des cas, les autorisations dont disposent déjà vos instances pour Bottlerocket couvrent également. GuardDuty Aucune politique supplémentaire n'est nécessaire. La `AmazonEC2ContainerRegistryReadOnly` politique utilisée par Bottlerocket pour récupérer ses images de conteneur de contrôle et d'administration répond également à l'exigence d'extraire l'image GuardDuty du conteneur de l'agent. Pour plus d'informations, consultez le fichier README de [Bottlerocket](#).

Le profil d'instance doit inclure les politiques gérées suivantes :

- `AmazonSSMManagedInstanceCore`— Nécessaire pour que le conteneur de contrôle Bottlerocket exécute l'agent SSM. Pour gérer vos instances Amazon EC2 avec Systems Manager, consultez la section [Configuration de Systems Manager pour les instances Amazon EC2](#) dans AWS Systems Manager le guide de l'utilisateur.
- `AmazonEC2ContainerRegistryReadOnly`— Nécessaire pour extraire l'image du conteneur de l' GuardDuty agent depuis Amazon ECR. Les autorisations suivantes sont requises au minimum :

```
...  
    "ecr:GetAuthorizationToken",  
    "ecr:BatchCheckLayerAvailability",  
    "ecr:GetDownloadUrlForLayer",  
    "ecr:BatchGetImage",  
...
```

Pour restreindre davantage les autorisations Amazon ECR, vous pouvez ajouter l'URI du référentiel Amazon ECR qui héberge l'agent de GuardDuty sécurité pour Amazon ECS-Amazon EC2 Bottlerocket. Pour plus d'informations, consultez [Référentiel ECR pour l' GuardDuty agent sur ECS-EC2 Bottlerocket](#).

Validation des exigences architecturales

L'architecture de vos instances détermine le comportement de l'agent GuardDuty de sécurité. Bottlerocket ECS-2 et ses ECS-3 variantes répondent à ces exigences dès le départ. Vérifiez les points suivants avant d'activer la surveillance du temps d'exécution :

- Le support du noyau inclut `eBPFTracepoints`, `etKprobe`. Les variantes de Bottlerocket utilisent le noyau 6.1 et ECS-3 les ECS-2 variantes utilisent le noyau. 6.12 Les deux versions répondent aux exigences du noyau pour la surveillance du temps d'exécution. L'option `CONFIG_DEBUG_INFO_BTF=y` kernel est activée par défaut dans Bottlerocket ECS-2 et kernels. ECS-3
- Pour les architectures CPU, Runtime Monitoring prend en charge AMD64 (x86_64) et ARM64 (`aarch64`).

Exigences en matière de connectivité réseau

GuardDuty héberge son agent de sécurité sous forme d'image de conteneur dans Amazon ECR. Vos instances ont donc besoin d'une connectivité réseau avec Amazon ECR pour l'extraire. En fonction de la configuration de votre réseau, choisissez l'une des options suivantes :

Option 1 - Utilisation de l'accès au réseau public (si disponible)

Si vos instances Bottlerocket s'exécutent dans des sous-réseaux dotés d'un accès Internet sortant, aucune configuration réseau supplémentaire n'est requise.

Option 2 - Utilisation des points de terminaison Amazon VPC (pour les sous-réseaux privés)

Pour les instances Bottlerocket situées dans des sous-réseaux privés, les points de terminaison VPC fournissent la connectivité dont l'agent a besoin. Configurez les points de terminaison pour Amazon ECR, Amazon S3 et Systems Manager afin que les instances puissent extraire l'image de l'agent et communiquer avec Systems Manager pour le déploiement.

Pour plus d'informations sur la configuration des points de terminaison VPC, consultez [Créer les points de terminaison VPC pour Amazon ECR dans le guide de l'utilisateur](#)

[d'Amazon Elastic Container Registry et créer des points de terminaison VPC](#) dans le guide de l'utilisateur.AWS Systems Manager

Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes

Si vous avez défini une politique de contrôle des services (SCP) pour gérer les autorisations dans votre organisation, vérifiez que la limite des autorisations autorise `!guardduty:SendSecurityTelemetryaction`. GuardDuty nécessite cette autorisation pour prendre en charge la surveillance du temps d'exécution sur différents types de ressources.

Si votre compte est un compte membre, contactez l'administrateur délégué associé. Pour plus d'informations sur la gestion des SCP pour votre organisation, voir [Politiques de contrôle des services \(SCP\)](#).

Lors de l'utilisation de la configuration automatique des agents

Pour utiliser la configuration automatique des agents, vous Compte AWS devez remplir les conditions préalables suivantes :

- Lorsque vous utilisez des balises d'inclusion avec une configuration d'agent automatisée, GuardDuty pour créer une association SSM pour une nouvelle instance, assurez-vous que la nouvelle instance est gérée par SSM et qu'elle apparaît sous Fleet Manager dans la <https://console.aws.amazon.com/systems-manager/console>.
- Lorsque vous utilisez des balises d'exclusion avec une configuration automatique de l'agent :
 - Ajoutez le `false` tag `GuardDutyManaged` : à une instance Amazon EC2 avant de la lancer et avant de configurer l'agent GuardDuty automatique pour votre compte. Une fois la configuration automatique des agents activée, toute instance lancée sans balise d'exclusion est automatiquement couverte.
 - Activez le paramètre Autoriser les balises dans les métadonnées pour vos instances. Ce paramètre est obligatoire car il GuardDuty faut lire la balise d'exclusion du service de métadonnées d'instance (IMDS) pour déterminer s'il doit exclure l'instance de l'installation de l'agent. Pour plus d'informations, consultez [Activer l'accès aux balises dans les métadonnées des instances](#) dans le guide de l'utilisateur Amazon EC2.

Limite du processeur et de la mémoire pour GuardDuty l'agent

Limite du processeur

GuardDuty limite l'agent de sécurité à 10 % de la capacité totale du vCPU de l'instance. Par exemple, sur une instance dotée de 4 cœurs de vCPU, l'agent peut utiliser au maximum 0,4 vCPU.

Limite de mémoire

En ce qui concerne la mémoire associée à votre instance Amazon EC2, la quantité de mémoire que l'agent de GuardDuty sécurité peut utiliser est limitée.

Le tableau suivant indique la limite de mémoire.

Mémoire de l'instance Amazon EC2	Mémoire maximale pour l' GuardDuty agent
Moins de 8 Go	128 Mo
8 Go à moins de 32 Go	256 Mo
Plus ou égal à 32 Go	1 Go

Étape suivante

L'étape suivante consiste à configurer la surveillance du temps d'exécution et à gérer automatiquement l'agent de sécurité.

Prérequis pour AWS Fargate (Amazon ECS uniquement) support

Cette section inclut les conditions préalables à la surveillance du comportement d'exécution de vos ressources Fargate-Amazon ECS. Une fois ces conditions préalables remplies, voir [Activer la surveillance du GuardDuty temps d'exécution](#).

Rubriques

- [Validation des exigences architecturales](#)
- [Conditions préalables à l'accès aux images du conteneur](#)
- [Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes](#)

- [Validation des autorisations des rôles et des limites des autorisations liées aux politiques](#)
- [Limites de processeur et de mémoire](#)

Validation des exigences architecturales

La plate-forme que vous utilisez peut avoir un impact sur GuardDuty la manière dont l'agent de sécurité prend GuardDuty en charge la réception des événements d'exécution de vos clusters Amazon ECS. Vous devez confirmer que vous utilisez l'une des plateformes vérifiées.

Considérations initiales :

La AWS Fargate plate-forme de vos clusters Amazon ECS doit être Linux. La version de plateforme correspondante doit être au moins 1.4.0, ou LATEST. Pour plus d'informations sur les versions de plate-forme, consultez les versions de la [plate-forme Linux](#) dans le manuel Amazon Elastic Container Service Developer Guide.

Les versions de la plateforme Windows ne sont pas encore prises en charge.

Pour les architectures de processeur, les distributions du système d'exploitation et les versions du noyau vérifiées, consultez [Architectures de processeur, systèmes d'exploitation et versions de noyau pris en charge](#).

Conditions préalables à l'accès aux images du conteneur

Les prérequis suivants vous permettent d'accéder à l'image du conteneur du GuardDuty sidecar depuis le référentiel Amazon ECR.

Conditions d'autorisation

Le rôle d'exécution des tâches nécessite certaines autorisations Amazon Elastic Container Registry (Amazon ECR) pour télécharger l'image du conteneur de GuardDuty l'agent de sécurité :

```
...
    "ecr:GetAuthorizationToken",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer",
    "ecr:BatchGetImage",
...
```

Pour restreindre davantage les autorisations Amazon ECR, vous pouvez ajouter l'URI du référentiel Amazon ECR qui héberge l'agent GuardDuty de sécurité pour (AWS Fargate Amazon ECS uniquement). Pour plus d'informations, consultez [Agent d'hébergement GuardDuty de référentiels Amazon ECR](#).

Vous pouvez utiliser la politique [AmazonECSTaskExecutionRolePolicy](#) gérée ou ajouter les autorisations ci-dessus à votre TaskExecutionRole politique.

Configuration de la définition des tâches

Lorsque vous créez ou mettez à jour des services Amazon ECS, vous devez fournir des informations de sous-réseau dans votre définition de tâche :

L'exécution des [UpdateService](#) API [CreateService](#) et dans la référence d'API Amazon Elastic Container Service nécessite que vous transmettiez les informations du sous-réseau. Pour plus d'informations, consultez les [définitions des tâches Amazon ECS](#) dans le manuel Amazon Elastic Container Service Developer Guide.

Exigences en matière de connectivité réseau

Vous devez vous assurer de la connectivité réseau pour télécharger l'image du GuardDuty conteneur depuis Amazon ECR. Cette exigence est spécifique au GuardDuty fait qu'il utilise Amazon ECR pour héberger son agent de sécurité. En fonction de la configuration de votre réseau, vous devez implémenter l'une des options suivantes :

Option 1 - Utilisation de l'accès au réseau public (si disponible)

Si vos tâches Fargate s'exécutent dans des sous-réseaux dotés d'un accès Internet sortant, aucune configuration réseau supplémentaire n'est requise.

Option 2 - Utilisation des points de terminaison Amazon VPC (pour les sous-réseaux privés)

Si vos tâches Fargate s'exécutent dans des sous-réseaux privés sans accès à Internet, vous devez configurer les points de terminaison VPC pour l'ECR afin de garantir que l'URI du référentiel ECR hébergeant l'agent de sécurité est accessible au réseau. GuardDuty Sans ces points de terminaison, les tâches des sous-réseaux privés ne peuvent pas télécharger l'image du GuardDuty conteneur.

Pour les instructions de configuration des points de terminaison VPC, consultez la section [Création des points de terminaison VPC pour Amazon ECR dans le guide de l'utilisateur d'Amazon](#) Elastic Container Registry.

Pour plus d'informations sur l'activation de Fargate pour télécharger GuardDuty le conteneur, consultez la section [Utilisation des images Amazon ECR avec Amazon ECS dans le guide de l'utilisateur d'Amazon Elastic Container Registry](#).

Configuration du groupe de sécurité

Les images du GuardDuty conteneur se trouvent dans Amazon ECR et nécessitent un accès Amazon S3. Cette exigence est spécifique au téléchargement d'images de conteneurs depuis Amazon ECR. Pour les tâches dont l'accès au réseau est restreint, vous devez configurer vos groupes de sécurité pour autoriser l'accès à S3.

Ajoutez une règle sortante dans votre groupe de sécurité qui autorise le trafic vers la [liste de préfixes gérés S3 \(p1-xxxxxxx\) sur le port 443](#). Pour ajouter une règle sortante, consultez la section [Configurer les règles des groupes de sécurité](#) dans le guide de l'utilisateur Amazon VPC.

Pour consulter vos listes de AWS préfixes gérées dans la console ou les décrire en utilisant AWS Command Line Interface (AWS CLI), consultez les listes de [préfixes AWS gérées par -dans le guide de l'utilisateur](#) Amazon VPC.

Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes

Cette section explique comment valider les paramètres de votre politique de contrôle des services (SCP) afin de garantir que la surveillance du temps d'exécution fonctionne comme prévu au sein de votre organisation.

Si vous avez défini une ou plusieurs politiques de contrôle des services pour gérer les autorisations dans votre organisation, vous devez vérifier qu'elle ne refuse pas l'`guardduty:SendSecurityTelemetryaction`. Pour plus d'informations sur le fonctionnement des SCP, voir l'[évaluation des SCP](#) dans le guide de l'AWS Organizations utilisateur.

Si votre compte est un compte membre, contactez l'administrateur délégué associé. Pour plus d'informations sur la gestion des SCP pour votre organisation, consultez la section [Politiques de contrôle des services \(SCP\)](#) dans le guide de l'AWS Organizations utilisateur.

Procédez comme suit pour tous les SCP que vous avez configurés dans votre environnement multi-comptes :

Pour valider le **devoir de garde** : `n:SendSecurityTelemetry` est pas refusé dans le SCP

1. Connectez-vous à la console Organizations à l'adresse <https://console.aws.amazon.com/organizations/>. Vous devez vous connecter en tant que rôle IAM ou en tant qu'utilisateur root ([ce n'est pas recommandé](#)) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, sélectionnez Politiques (politiques). Ensuite, sous Types de politiques pris en charge, sélectionnez Politiques de contrôle des services.
3. Sur la page Politiques de contrôle des services, choisissez le nom de la politique que vous souhaitez valider.
4. Sur la page détaillée de la politique, consultez le contenu de cette politique. Assurez-vous qu'il ne refuse pas `guardduty:SendSecurityTelemetry`.

La politique SCP suivante est un exemple pour ne pas nier `guardduty:SendSecurityTelemetry` :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:SendSecurityTelemetry"
      ],
      "Resource": "*"
    }
  ]
}
```

Si votre politique refuse cette action, vous devez la mettre à jour. Pour plus d'informations, consultez [Mise à jour d'une politique de contrôle des services \(SCP\)](#) dans le Guide de l'utilisateur AWS Organizations .

Validation des autorisations des rôles et des limites des autorisations liées aux politiques

Suivez les étapes suivantes pour vérifier que les limites d'autorisations associées au rôle et à sa politique ne limitent pas `guardduty:SendSecurityTelemetry` l'action.

Pour afficher la limite des autorisations pour les rôles et sa politique

1. Connectez-vous à la console IAM Console de gestion AWS et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles.
3. Sur la page Rôles, sélectionnez le rôle *TaskExecutionRole* que vous avez peut-être créé.
4. Sur la page du rôle sélectionné, sous l'onglet Autorisations, développez le nom de la politique associée à ce rôle. Vérifiez ensuite que cette politique ne restreint pas `guardduty:SendSecurityTelemetry`.
5. Si la limite des autorisations est définie, développez cette section. Ensuite, développez chaque politique pour vérifier qu'elle ne limite pas l'action `guardduty:SendSecurityTelemetry`. La politique doit ressembler à cela [Exemple SCP policy](#).

Le cas échéant, effectuez l'une des actions suivantes :

- Pour modifier la politique, sélectionnez Modifier. Sur la page Modifier les autorisations pour cette politique, mettez-la à jour dans l'éditeur de stratégie. Assurez-vous que le schéma JSON reste valide. Ensuite, choisissez Suivant. Vous pouvez ensuite consulter et enregistrer les modifications.
- Pour modifier cette limite d'autorisations et en choisir une autre, choisissez Modifier la limite.
- Pour supprimer cette limite d'autorisations, choisissez Supprimer la limite.

Pour plus d'informations sur la gestion des politiques, consultez la section [Politiques et autorisations Gestion des identités et des accès AWS dans](#) le guide de l'utilisateur IAM.

Limites de processeur et de mémoire

Dans la définition de la tâche Fargate, vous devez spécifier la valeur du processeur et de la mémoire au niveau de la tâche. Le tableau suivant indique les combinaisons valides de valeurs de processeur

et de mémoire au niveau des tâches, ainsi que la limite de mémoire maximale de l'agent de GuardDuty sécurité correspondant pour le GuardDuty conteneur.

Valeur d'UC	Valeur de mémoire	GuardDuty limite de mémoire maximale de l'agent
256 (0,25 vCPU)	512 MiB, 1 Go, 2 Go	128 Mo
512 (0,5 vCPU)	1 Go, 2 Go, 3 Go, 4 Go	
1 024 (1 vCPU)	2 Go, 3 Go, 4 Go	
	5 Go, 6 Go, 7 Go, 8 Go	
2 048 (2 vCPU)	Entre 4 Go et 16 Go par incréments de 1 Go	
4 096 (4 vCPU)	Entre 8 Go et 20 Go par incréments de 1 Go	
8192 (8 vCPU)	Entre 16 Go et 28 Go par incréments de 4 Go	256 Mo
	Entre 32 Go et 60 Go par incréments de 4 Go	512 Mo
16384 (16 vCPU)	Entre 32 Go et 120 Go par incréments de 8 Go	1 Go

Après avoir activé la surveillance du temps d'exécution et vérifié que l'état de couverture de votre cluster est sain, vous pouvez configurer et consulter les métriques Container Insight. Pour plus d'informations, consultez [Configuration de la surveillance sur le cluster Amazon ECS](#).

L'étape suivante consiste à configurer la surveillance du temps d'exécution ainsi que l'agent de sécurité.

Conditions préalables à la prise en charge des clusters Amazon EKS

Cette section inclut les conditions préalables à la surveillance du comportement d'exécution de vos ressources Amazon EKS. Ces conditions préalables sont cruciales pour que l'agent GuardDuty fonctionne comme prévu. Une fois ces conditions préalables remplies, consultez [Activer la surveillance du GuardDuty temps d'exécution](#) pour commencer à surveiller vos ressources.

Support pour les fonctionnalités d'Amazon EKS

La surveillance du temps d'exécution prend en charge les clusters Amazon EKS exécutés sur des instances Amazon EC2 et le mode automatique Amazon EKS.

La surveillance du temps d'exécution ne prend pas en charge les clusters Amazon EKS dotés de nœuds hybrides Amazon EKS, ni ceux qui s'exécutent sur AWS Fargate.

Pour plus d'informations sur ces fonctionnalités d'Amazon EKS, consultez [Qu'est-ce qu'Amazon EKS ?](#) dans le guide de l'utilisateur Amazon EKS.

Validation des exigences architecturales

La plate-forme que vous utilisez peut avoir un impact sur GuardDuty la manière dont l'agent de sécurité prend GuardDuty en charge la réception des événements d'exécution de vos clusters EKS. Vous devez confirmer que vous utilisez l'une des plateformes vérifiées. Si vous gérez l'agent GuardDuty manuellement, assurez-vous que la version de Kubernetes prend en charge la version de l'agent GuardDuty actuellement utilisée.

Plateformes vérifiées

Pour les architectures de processeur, les distributions du système d'exploitation et les versions du noyau vérifiées, consultez [Architectures de processeur, systèmes d'exploitation et versions de noyau pris en charge](#).

Actuellement, avec la version du noyau 5.4 dans ARM64 (aarch64), je ne GuardDuty peux pas générer ceux [GuardDuty Types de recherche liés à la surveillance du temps](#) qui sont liés à [Événements du système de noms de domaine \(DNS\)](#).

Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty

Le tableau suivant indique les versions de Kubernetes pour vos clusters EKS prises en charge par GuardDuty l'agent de sécurité.

Version de l'agent GuardDuty de sécurité complémentaire Amazon EKS	Version de Kubernetes
v1.17.1 (dernière version - v1.17.1-eksbuild.2)	1,31 - 1,36
v1.16.0 (dernière version - v1.16.0-eksbuild.2)	1,28 - 1,36
v1.15.0 (dernière version - v1.15.0-eksbuild.2)	1,28 - 1,36
v1.12.2 (dernière version - v1.12.2-eksbuild.2)	1,28 - 1,36
v1.12.1 (dernière version - v1.12.1-eksbuild.4)	1,28 - 1,35
v1.11.0 (dernière version - v1.11.0-eksbuild.4)	1,28 - 1,34
v1.10.0 (dernière version - v1.10.0-eksbuild.2)	1,21 - 1,33
v1.9.0 (dernière version - v1.9.0-eksbuild.2)	1,21 - 1,32
v1.8.1 (dernière version - v1.8.1-eksbuild.2)	
v1.7.1	1,21 - 1,31
v1.7.0	
v1.6.1	
v1.6.0	1,21 - 1,29
v1.5.0	
v1.4.1	
v1.4.0	
v1.3.1	
v1.3.0	1,21 - 1,28
v1.2.0	
v1.1.0	1,21 - 1,26

Version de l'agent GuardDuty de sécurité complémentaire Amazon EKS	Version de Kubernetes
v1.0.0	1,21 - 1,25

Certaines versions de l'agent GuardDuty de sécurité atteindront la fin du support standard.

Pour plus d'informations sur les versions publiées de l'agent, consultez [GuardDuty versions de l'agent de sécurité pour les ressources Amazon EKS](#).

Limites de processeur et de mémoire

Le tableau suivant indique les limites de processeur et de mémoire pour le module complémentaire Amazon EKS pour GuardDuty (aws-guardduty-agent).

Paramètre	Limite minimum	Limite maximum
CPU	200 m	1 000 m
Mémoire	256 milles	1 024 milles

Lorsque vous utilisez le module complémentaire Amazon EKS version 1.5.0 ou supérieure, il GuardDuty permet de configurer le schéma du module complémentaire pour les valeurs de votre processeur et de votre mémoire. Pour plus d'informations sur la plage configurable, consultez [Paramètres et valeurs configurables](#).

Une fois que vous avez activé la surveillance d'exécution EKS et évalué l'état de couverture de vos clusters EKS, vous pouvez configurer et consulter les métriques d'aperçu des conteneurs. Pour plus d'informations, consultez [Configuration de la surveillance du processeur et de la mémoire](#).

Validation de la politique de contrôle des services de votre organisation

Si vous avez défini une politique de contrôle des services (SCP) pour gérer les autorisations dans votre organisation, vérifiez que la limite des autorisations n'est pas restrictive `guardduty:SendSecurityTelemetry`. GuardDuty nécessite cette autorisation pour prendre en charge la surveillance du temps d'exécution sur différents types de ressources.

Si votre compte est un compte membre, contactez l'administrateur délégué associé. Pour plus d'informations sur la gestion des SCP pour votre organisation, voir [Politiques de contrôle des services \(SCP\)](#).

Architectures de processeur, systèmes d'exploitation et versions de noyau pris en charge

Cette section consolide les architectures de processeur, les distributions du système d'exploitation et les versions du noyau qui ont été vérifiées pour prendre en charge l'agent GuardDuty de sécurité. À moins qu'un type de ressource ne soit appelé séparément, ces exigences s'appliquent à la surveillance du temps d'exécution pour les instances Amazon EC2 (AWS Fargate Amazon ECS uniquement) et les clusters Amazon EKS.

Le support du noyau inclut eBPFTracepoints, etKprobe. Pour les architectures CPU, Runtime Monitoring prend en charge AMD64 (x64) et ARM64 (Graviton2 et versions ultérieures). ¹

Le tableau suivant indique les distributions du système d'exploitation et les versions du noyau dont la prise en charge de l'agent de GuardDuty sécurité a été vérifiée.

Distribution du système d'exploitation ²	Version du noyau ³
Amazon Linux 2	5,4 ⁴ , 5,10 ⁴ , 5,15
Amazon Linux 2023	5,4 ⁴ , 5,10 ⁴ , 5,15, 6,1, 6,5, 6,8, 6,12
Ubuntu 20,04, 22,04, 24,04, 26,04	5,4 ⁴ , 5,10 ⁴ , 5,15, 6,1, 6,5, 6,8, 6,13, 6,14, 6,15, 6,16, 6,17, 6,18, 7,0
Debian 11, 12, 13	5,4 ⁴ , 5,10 ⁴ , 5,15, 6,1, 6,5, 6,8, 6,12
RedHat 9,4, 10,2	5,14, 6,12
Fedora 34, 40, 41, 43, 44	5,11, 5,17, 6,8, 6,12, 7,1
CentOS Stream 9, 10	5,14, 6,12
Oracle Linux 8.9, 9.3	5,15

Distribution du système d'exploitation ²	Version du noyau ³
Rocky Linux 9.5, 10.1	5,14, 6,12
Alma Linux 9, 10	5,14, 6,12
Serveur SUSE Linux Enterprise 16	6,12
Flacon Rocket	5,4 ⁴ , 5,10 ⁴ , 5,15, 6,1, 6,18

1. Runtime Monitoring ne prend pas en charge les instances Graviton de première génération telles que les types d'instances A1.
2. Support pour différents systèmes d'exploitation : la prise en charge de la surveillance du temps d'exécution GuardDuty a été vérifiée pour la distribution d'exploitation répertoriée dans le tableau précédent. Bien que l'agent GuardDuty de sécurité puisse s'exécuter sur des systèmes d'exploitation non répertoriés dans le tableau précédent, l' GuardDuty équipe ne peut garantir la valeur de sécurité attendue.
3. Quelle que soit la version du noyau, vous devez définir l'CONFIG_DEBUG_INFO_BTFindicateur sur y (c'est-à-dire vrai). Cela est nécessaire pour que l'agent GuardDuty de sécurité puisse fonctionner comme prévu.

Pour AWS Fargate (Amazon ECS uniquement), cette option de noyau est gérée par Fargate et ne nécessite aucune action de votre part.

4. Pour les versions 5.10 et antérieures du noyau, l'agent GuardDuty de sécurité utilise de la mémoire verrouillée dans RAM (RLIMIT_MEMLOCK) pour fonctionner comme prévu. Si la RLIMIT_MEMLOCK valeur de votre système est trop faible, il est GuardDuty recommandé de définir des limites strictes et souples à au moins 32 Mo. Pour plus d'informations sur la vérification et la modification de la RLIMIT_MEMLOCK valeur par défaut sur les instances Amazon EC2, consultez. [Affichage et mise à jour des valeurs RLIMIT_MEMLOCK](#)

Activer la surveillance du GuardDuty temps d'exécution

Avant d'activer la surveillance du temps d'exécution dans votre compte, assurez-vous que le type de ressource pour lequel vous souhaitez surveiller les événements d'exécution répond aux exigences de la plate-forme. Pour plus d'informations, consultez [Conditions préalables](#).

Si vous utilisiez EKS Runtime Monitoring avant le lancement de Runtime Monitoring, vous pouvez utiliser les API pour vérifier et mettre à jour la configuration existante pour EKS Runtime Monitoring. Vous pouvez également migrer votre configuration existante d'EKS Runtime Monitoring vers Runtime Monitoring. Pour plus d'informations, consultez [Migration de la surveillance d'exécution EKS vers la surveillance d'exécution](#).

Note

À l'heure actuelle, cette documentation fournit les étapes permettant d'activer la surveillance du temps d'exécution pour vos comptes et votre organisation par console uniquement. Vous pouvez également activer la surveillance du temps d'exécution à l'aide [des actions d'API](#) ou [AWS CLI pour GuardDuty](#).

Vous pouvez configurer la surveillance du temps d'exécution en suivant les étapes décrites dans les rubriques suivantes.

Table des matières

- [Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples](#)
- [Activation de la surveillance du temps d'exécution pour un compte autonome](#)

Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples

Dans les environnements à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la surveillance du temps d'exécution pour les comptes des membres et gérer la configuration automatique des agents pour les types de ressources appartenant aux comptes membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter [Managing multiple accounts](#).

Pour le compte GuardDuty d'administrateur délégué

Pour activer la surveillance du temps d'exécution pour le compte GuardDuty administrateur délégué

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sous l'onglet Configuration, choisissez Modifier dans la section Configuration de la surveillance du temps d'exécution.
4. Utilisation d'Activer pour tous les comptes

Si vous souhaitez activer la surveillance du temps d'exécution pour tous les comptes appartenant à l'organisation, y compris le compte d' GuardDuty administrateur délégué, choisissez Activer pour tous les comptes.

5. Utilisation de Configurer les comptes manuellement

Si vous souhaitez activer la surveillance du temps d'exécution pour chaque compte membre individuellement, choisissez Configurer les comptes manuellement.

- Choisissez Activer sous la section Administrateur délégué (ce compte).

6. Gérez l'agent de sécurité correspondant à votre type de ressource. Pour plus d'informations, consultez [Gestion des agents GuardDuty de sécurité](#).

Pour tous les comptes de membres

Pour activer la surveillance du temps d'exécution pour tous les comptes membres de l'organisation

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide du compte GuardDuty d'administrateur délégué.

2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sur la page Runtime Monitoring, sous l'onglet Configuration, choisissez Modifier dans la section Configuration de Runtime Monitoring.
4. Choisissez Activer pour tous les comptes.
5. Gérez l'agent de sécurité correspondant à votre type de ressource. Pour plus d'informations, consultez [Gestion des agents GuardDuty de sécurité](#).

Pour tous les comptes de membres actifs existants

Pour activer la surveillance du temps d'exécution pour les comptes membres existants de l'organisation

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide du compte GuardDuty d'administrateur délégué de l'organisation.

2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sur la page Runtime Monitoring, sous l'onglet Configuration, vous pouvez consulter l'état actuel de la configuration Runtime Monitoring.
4. Dans le volet Runtime Monitoring, dans la section Comptes membres actifs, sélectionnez Actions.
5. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
6. Choisissez Confirmer.
7. Gérez l'agent de sécurité correspondant à votre type de ressource. Pour plus d'informations, consultez [Gestion des agents GuardDuty de sécurité](#).

Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Auto-enable Surveillance du temps d'exécution pour les nouveaux comptes membres uniquement

Pour activer la surveillance du temps d'exécution pour les nouveaux comptes membres de votre organisation

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide du compte d'administrateur délégué désigné par l'organisation.

2. Dans le volet de navigation, choisissez Runtime Monitoring

3. Sous l'onglet Configuration, choisissez Modifier dans la section Configuration de la surveillance du temps d'exécution.
4. Choisissez Configurer les comptes manuellement.
5. Sélectionnez Activer automatiquement pour les nouveaux comptes membres.
6. Gérez l'agent de sécurité correspondant à votre type de ressource. Pour plus d'informations, consultez [Gestion des agents GuardDuty de sécurité](#).

Pour les comptes de membres actifs sélectionnés uniquement

Pour activer la surveillance du temps d'exécution pour les comptes de membres actifs individuels

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sur la page Comptes, passez en revue les valeurs des colonnes Runtime Monitoring et Manage automatique de l'agent. Ces valeurs indiquent si la surveillance du temps d'exécution et la gestion des GuardDuty agents sont activées ou non pour le compte correspondant.
4. Dans le tableau Comptes, sélectionnez le compte pour lequel vous souhaitez activer la surveillance du temps d'exécution. Vous pouvez choisir plusieurs comptes à la fois.
5. Choisissez Confirmer.
6. Choisissez Modifier les plans de protection. Choisissez l'action appropriée.
7. Choisissez Confirmer.
8. Gérez l'agent de sécurité correspondant à votre type de ressource. Pour plus d'informations, consultez [Gestion des agents GuardDuty de sécurité](#).

Activation de la surveillance du temps d'exécution pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour plus

d'informations, consultez [Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples](#).

Après avoir activé la surveillance du temps d'exécution, veillez à installer l'agent GuardDuty de sécurité par le biais d'une configuration automatique ou d'un déploiement manuel. Dans le cadre de toutes les étapes répertoriées dans la procédure suivante, veillez à installer l'agent de sécurité.

Pour activer la surveillance du temps d'exécution dans un compte autonome

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Dans l'onglet Configuration, choisissez Activer pour activer la surveillance du temps d'exécution pour votre compte.
4. Gérez l'agent de sécurité correspondant à votre type de ressource. Pour plus d'informations, consultez [Gestion des agents GuardDuty de sécurité](#).

Gestion des agents GuardDuty de sécurité

Vous pouvez gérer l'agent GuardDuty de sécurité pour la ressource que vous souhaitez surveiller. Si vous souhaitez surveiller plusieurs types de ressources, assurez-vous de gérer l'agent GuardDuty correspondant à cette ressource.

Les rubriques suivantes vous aideront à suivre les prochaines étapes de gestion de l'agent de sécurité.

Table des matières

- [Activation de l'agent de sécurité automatique pour l'instance Amazon EC2](#)
- [Gestion manuelle de l'agent de sécurité pour la ressource Amazon EC2](#)
- [Gestion GuardDuty de l'agent de sécurité sur Bottlerocket \(Amazon ECS sur Amazon EC2\)](#)
- [Gestion de l'agent de sécurité automatisé pour Fargate \(Amazon ECS uniquement\)](#)
- [Gestion automatique de l'agent de sécurité pour les ressources Amazon EKS](#)
- [Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS](#)
- [Configuration des paramètres GuardDuty de l'agent de sécurité \(module complémentaire\) pour Amazon EKS](#)
- [Validation de la configuration des points de terminaison VPC](#)

Activation de l'agent de sécurité automatique pour l'instance Amazon EC2

Cette section décrit les étapes à suivre pour activer l'agent GuardDuty automatique pour vos ressources Amazon EC2 dans votre compte autonome ou dans un environnement à comptes multiples.

Avant de continuer, assurez-vous de suivre toutes les [Conditions préalables à la prise en charge des instances Amazon EC2](#).

Rubriques

- [GuardDuty Agent d'activation pour les ressources Amazon EC2 dans un environnement multi-comptes](#)
- [Activation d'un agent GuardDuty automatisé pour les ressources Amazon EC2 dans un compte autonome](#)
- [Migration d'un agent manuel Amazon EC2 vers un agent automatisé](#)

Si vous passez de la gestion manuelle de l'agent GuardDuty à l'activation de l'agent GuardDuty automatisé, avant de suivre les étapes d'activation de l'agent GuardDuty automatisé, consultez [Migration d'un agent manuel Amazon EC2 vers un agent automatisé](#).

GuardDuty Agent d'activation pour les ressources Amazon EC2 dans un environnement multi-comptes

Dans les environnements à comptes multiples, seul le compte d'administrateur délégué GuardDuty peut activer ou désactiver la configuration automatique des agents pour les types de ressources appartenant aux comptes des membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d'administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter [Managing multiple accounts](#).

Pour le compte GuardDuty d'administrateur délégué

Configure for all instances

Si vous avez choisi Activer pour tous les comptes pour la surveillance du temps d'exécution, choisissez l'une des options suivantes pour le compte d'administrateur délégué :

- Option 1

Sous Configuration automatique de l'agent, dans la section EC2, sélectionnez Activer pour tous les comptes.

- Option 2
 - Sous Configuration automatique de l'agent, dans la section EC2, sélectionnez Configurer les comptes manuellement.
 - Sous Administrateur délégué (ce compte), choisissez Activer.
- Cliquez sur Enregistrer.

Si vous avez choisi Configurer les comptes manuellement pour la surveillance du temps d'exécution, effectuez les étapes suivantes :

- Sous Configuration automatique de l'agent, dans la section EC2, sélectionnez Configurer les comptes manuellement.
- Sous Administrateur délégué (ce compte), choisissez Activer.
- Cliquez sur Enregistrer.

Quelle que soit l'option que vous choisissiez pour activer la configuration automatique de l'agent pour le compte d' GuardDuty administrateur délégué, vous pouvez vérifier que l'association SSM GuardDuty créée installera et gèrera l'agent de sécurité sur toutes les ressources EC2 appartenant à ce compte.

1. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
2. Ouvrez l'onglet Targets pour l'association SSM (GuardDutyRuntimeMonitoring-do-not-delete). Notez que la touche Tag apparaît sous la forme Instancelds.

Using inclusion tag in selected instances

Pour configurer GuardDuty l'agent pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. Ajoutez la true balise GuardDutyManaged : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).

L'ajout de cette balise permettra GuardDuty d'installer et de gérer l'agent de sécurité pour ces instances EC2 sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.

3. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gèrera l'agent de sécurité uniquement sur les ressources EC2 étiquetées avec les balises d'inclusion.

Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.

- Ouvrez l'onglet Targets pour l'association SSM créée (GuardDutyRuntimeMonitoring-do-not-delete). La touche Tag apparaît sous la forme de tag : GuardDutyManaged.

Using exclusion tag in selected instances

Note

Assurez-vous d'ajouter la balise d'exclusion à vos instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer GuardDuty l'agent pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. Ajoutez la fa lse balise GuardDutyManaged : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).
3. Pour [des balises d'exclusion seront disponibles](#) dans les métadonnées de l'instance, effectuez les étapes suivantes :
 - a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.

- b. Dans le menu Actions, sélectionnez Paramètres de l'instance.
 - c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécution [Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2](#).

Auto-enable pour tous les comptes membres

 Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Configure for all instances

Les étapes suivantes supposent que vous avez choisi Activer pour tous les comptes dans la section Runtime Monitoring :

1. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent pour Amazon EC2.
2. Vous pouvez vérifier que l'association SSM qui GuardDuty crée (GuardDutyRuntimeMonitoring-do-not-delete) installera et gèrera l'agent de sécurité sur toutes les ressources EC2 appartenant à ce compte.
 - a. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
 - b. Ouvrez l'onglet Targets pour l'association SSM. Notez que la touche Tag apparaît sous la forme Instancelds.

Using inclusion tag in selected instances

Pour configurer GuardDuty l'agent pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>
2. Ajoutez la true balise GuardDutyManaged : aux instances EC2 que vous souhaitez surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).

L'ajout de cette balise permettra GuardDuty d'installer et de gérer l'agent de sécurité pour ces instances EC2 sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.

3. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gèrera l'agent de sécurité sur toutes les ressources EC2 appartenant à votre compte.
 - a. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
 - b. Ouvrez l'onglet Targets pour l'association SSM (GuardDutyRuntimeMonitoring-do-not-delete). Notez que la touche Tag apparaît sous la forme Instancelds.

Using exclusion tag in selected instances

Note

Assurez-vous d'ajouter la balise d'exclusion à vos instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>
2. Ajoutez la false balise GuardDutyManaged : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).

3. Pour [des balises d'exclusion seront disponibles](#) dans les métadonnées de l'instance, effectuez les étapes suivantes :
 - a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.
 - b. Dans le menu Actions, sélectionnez Paramètres de l'instance.
 - c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécution [Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2](#).

Auto-enable pour les nouveaux comptes de membres uniquement

Le compte d' GuardDuty administrateur délégué peut définir la configuration automatique de l'agent pour la ressource Amazon EC2 afin de l'activer automatiquement pour les nouveaux comptes membres lorsqu'ils rejoignent l'organisation.

Configure for all instances

Les étapes suivantes supposent que vous avez sélectionné Activer automatiquement les nouveaux comptes membres dans la section Runtime Monitoring :

1. Dans le volet de navigation, choisissez Runtime Monitoring.
2. Sur la page Runtime Monitoring, choisissez Modifier.
3. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la configuration automatique des agents pour Amazon EC2 sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette sélection.
4. Cliquez sur Enregistrer.

Lorsqu'un nouveau compte membre rejoint l'organisation, cette configuration est automatiquement activée pour lui. GuardDuty Pour gérer l'agent de sécurité pour les instances Amazon EC2 qui appartiennent à ce nouveau compte membre, assurez-vous que toutes les conditions préalables sont remplies [Pour l'instance EC2](#).

Lorsqu'une association SSM est créée (GuardDutyRuntimeMonitoring-do-not-delete), vous pouvez vérifier qu'elle installera et gèrera l'agent de sécurité sur toutes les instances EC2 appartenant au nouveau compte membre.

- Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
- Ouvrez l'onglet Targets pour l'association SSM. Notez que la touche Tag apparaît sous la forme Instancelds.

Using inclusion tag in selected instances

Pour configurer l'agent GuardDuty de sécurité pour les instances sélectionnées de votre compte

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. Ajoutez la true balise GuardDutyManaged : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).

L'ajout de cette balise permettra GuardDuty d'installer et de gérer l'agent de sécurité pour ces instances sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.

3. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gèrera l'agent de sécurité uniquement sur les ressources EC2 étiquetées avec les balises d'inclusion.
 - a. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
 - b. Ouvrez l'onglet Targets pour l'association SSM créée. La touche Tag apparaît sous la forme de tag : GuardDutyManaged.

Using exclusion tag in selected instances

Note

Assurez-vous d'ajouter la balise d'exclusion à vos instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour des instances spécifiques de votre compte autonome

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. Ajoutez la fa lse balise GuardDutyManaged : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).
3. Pour [des balises d'exclusion seront disponibles](#) dans les métadonnées de l'instance, effectuez les étapes suivantes :
 - a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.
 - b. Dans le menu Actions, sélectionnez Paramètres de l'instance.
 - c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécution [Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2](#).

Comptes de membres sélectifs uniquement

Configure for all instances

1. Sur la page Comptes, sélectionnez un ou plusieurs comptes pour lesquels vous souhaitez activer la configuration de Monitoring-Automated l'agent Runtime (Amazon EC2). Assurez-vous que la surveillance du temps d'exécution est déjà activée sur les comptes que vous sélectionnez au cours de cette étape.
2. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration de Monitoring-Automated l'agent Runtime (Amazon EC2).
3. Choisissez Confirmer.

Using inclusion tag in selected instances

Pour configurer l'agent GuardDuty de sécurité pour les instances sélectionnées

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. Ajoutez la true balise GuardDutyManaged : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).

L'ajout de cette balise permettra GuardDuty de gérer l'agent de sécurité pour vos instances Amazon EC2 balisées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents (Runtime Monitoring - Automated agent Configuration (EC2)).

Using exclusion tag in selected instances

Note

Assurez-vous d'ajouter la balise d'exclusion à vos instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour les instances sélectionnées

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse.
<https://console.aws.amazon.com/ec2/>
2. Ajoutez la fa~~l~~se balise GuardDutyManaged : aux instances EC2 que vous ne souhaitez pas GuardDuty surveiller ou détecter de menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).
3. Pour [des balises d'exclusion seront disponibles](#) dans les métadonnées de l'instance, effectuez les étapes suivantes :
 - a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.
 - b. Dans le menu Actions, sélectionnez Paramètres de l'instance.
 - c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez maintenant évaluer [Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2](#).

Activation d'un agent GuardDuty automatisé pour les ressources Amazon EC2 dans un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour plus d'informations, consultez [Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples](#).

Après avoir activé la surveillance du temps d'exécution, veillez à installer l'agent GuardDuty de sécurité par le biais d'une configuration automatique ou d'un déploiement manuel. Dans le cadre de toutes les étapes répertoriées dans la procédure suivante, veillez à installer l'agent de sécurité.

Selon votre préférence en matière de surveillance de toutes les ressources Amazon EC2 ou de certaines d'entre elles, choisissez une méthode préférée et suivez les étapes décrites dans le tableau suivant.

Configure for all instances

Pour configurer la surveillance du temps d'exécution pour toutes les instances de votre compte autonome

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Dans l'onglet Configuration, choisissez Modifier.
4. Dans la section EC2, choisissez Enable.
5. Cliquez sur Enregistrer.
6. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gèrera l'agent de sécurité sur toutes les ressources EC2 appartenant à votre compte.
 - a. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
 - b. Ouvrez l'onglet Targets pour l'association SSM (GuardDutyRuntimeMonitoring-do-not-delete). Notez que la touche Tag apparaît sous la forme Instancelds.

Using inclusion tag in selected instances

Pour configurer l'agent GuardDuty de sécurité pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>
2. Ajoutez la true balise GuardDutyManaged : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).
3. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gèrera l'agent de sécurité uniquement sur les ressources EC2 étiquetées avec les balises d'inclusion.

Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.

- Ouvrez l'onglet Targets pour l'association SSM créée (GuardDutyRuntimeMonitoring-do-not-delete). La touche Tag apparaît sous la forme de tag : GuardDutyManaged.

Using exclusion tag in selected instances

Note

Assurez-vous d'ajouter la balise d'exclusion à vos instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. Ajoutez la fa lse balise GuardDutyManaged : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir [Pour ajouter une balise à une ressource individuelle](#).
3. Pour [des balises d'exclusion seront disponibles](#) dans les métadonnées de l'instance, effectuez les étapes suivantes :
 - a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.
 - b. Sélectionnez l'instance pour laquelle vous souhaitez autoriser les balises.
 - c. Dans le menu Actions, sélectionnez Paramètres de l'instance.
 - d. Choisissez Autoriser les balises dans les métadonnées de l'instance.
 - e. Sous Accès aux balises dans les métadonnées de l'instance, sélectionnez Autoriser.
 - f. Cliquez sur Enregistrer.

- Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécution [Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2](#).

Migration d'un agent manuel Amazon EC2 vers un agent automatisé

Cette section s'applique à vous Compte AWS si vous gériez auparavant l'agent de sécurité manuellement et que vous souhaitez maintenant utiliser la configuration GuardDuty automatique de l'agent. Si cela ne vous concerne pas, poursuivez la configuration de l'agent de sécurité pour votre compte.

Lorsque vous activez l'agent GuardDuty automatique, GuardDuty gère l'agent de sécurité en votre nom. Pour plus d'informations sur les étapes GuardDuty à suivre, consultez [Configuration automatique de l'agent \(recommandée\)](#).

nettoyer des ressources ;

Supprimer l'association SSM

- Supprimez toute association SSM que vous avez peut-être créée lorsque vous gériez manuellement l'agent de sécurité pour Amazon EC2. Pour plus d'informations, consultez la section [Suppression d'associations](#).
- Cela GuardDuty permet de prendre en charge la gestion des actions SSM, que vous utilisiez des agents automatisés au niveau du compte ou de l'instance (en utilisant des balises d'inclusion ou d'exclusion). Pour plus d'informations sur les actions que le SSM peut GuardDuty effectuer, consultez [Service-linked autorisations de rôle pour GuardDuty](#).
- Lorsque vous supprimez une association SSM précédemment créée pour gérer manuellement l'agent de sécurité, il peut y avoir une brève période de chevauchement lors de la GuardDuty création d'une association SSM pour gérer automatiquement l'agent de sécurité. Au cours de cette période, vous pourriez rencontrer des conflits liés à la planification SSM. Pour plus d'informations, consultez la section [Planification Amazon EC2 SSM](#).

Gérez les balises d'inclusion et d'exclusion pour vos instances Amazon EC2

- Balises d'inclusion — Lorsque vous n'activez pas la configuration GuardDuty automatique des agents mais que vous balisez l'une de vos instances Amazon EC2 avec une balise d'inclusion (GuardDutyManaged:true), vous GuardDuty créez une association SSM qui installera et

gèrera l'agent de sécurité sur les instances EC2 sélectionnées. Il s'agit d'un comportement attendu qui vous permet de gérer l'agent de sécurité uniquement sur certaines instances EC2. Pour plus d'informations, consultez [Déploiement de l'agent de sécurité sur Amazon EC2](#).

Pour GuardDuty empêcher l'installation et la gestion de l'agent de sécurité, supprimez la balise d'inclusion de ces instances EC2. Pour plus d'informations, consultez la section [Ajouter et supprimer des balises](#) dans le guide de l'utilisateur Amazon EC2.

- Balises d'exclusion : lorsque vous souhaitez activer la configuration GuardDuty automatique des agents pour toutes les instances EC2 de votre compte, assurez-vous qu'aucune instance EC2 n'est étiquetée avec une balise d'exclusion (GuardDutyManaged:false).

Gestion manuelle de l'agent de sécurité pour la ressource Amazon EC2

Cette section décrit les étapes à suivre pour installer et mettre à jour manuellement l'agent de sécurité pour vos ressources Amazon EC2.

Après avoir activé la surveillance du temps d'exécution, vous devez installer l'agent GuardDuty de sécurité manuellement. Pour gérer l'agent GuardDuty de sécurité manuellement, vous devez d'abord créer manuellement un point de terminaison Amazon VPC. Ensuite, vous pouvez installer l'agent de sécurité afin qu'il commence à GuardDuty recevoir les événements d'exécution des instances Amazon EC2. Lorsque vous GuardDuty publiez une nouvelle version d'agent pour cette ressource, vous pouvez mettre à jour la version de l'agent dans votre compte.

Les rubriques suivantes décrivent les étapes à suivre pour gérer en permanence l'agent de sécurité pour vos ressources Amazon EC2.

Rubriques

- [Prérequis — Création manuelle d'un point de terminaison Amazon VPC](#)
- [Installation manuelle de l'agent de sécurité](#)
- [Mise à jour manuelle GuardDuty de l'agent de sécurité pour l'instance Amazon EC2](#)

Prérequis — Création manuelle d'un point de terminaison Amazon VPC

Avant de pouvoir installer l'agent GuardDuty de sécurité, vous devez créer un point de terminaison Amazon Virtual Private Cloud (Amazon VPC). Cela vous aidera à GuardDuty recevoir les événements d'exécution de vos instances Amazon EC2.

 Note

L'utilisation du point de terminaison VPC n'entraîne aucun coût supplémentaire.

Pour créer un point de terminaison Amazon VPC

1. Connectez-vous à la console Amazon VPC Console de gestion AWS et ouvrez-la à l'adresse.
<https://console.aws.amazon.com/vpc/>
2. Dans le volet de navigation, sous Cloud privé VPC, sélectionnez Endpoints.
3. Choisissez Créer un point de terminaison.
4. Sur la page Créer un point de terminaison, pour Catégorie de services, choisissez Autres services de points de terminaison.
5. Pour Nom du service, entrez **com.amazonaws.us-east-1.guardduty-data**.

Assurez-vous de le remplacer **us-east-1** par votre Région AWS. Il doit s'agir de la même région que l'instance Amazon EC2 associée à votre identifiant de AWS compte.

6. Choisissez Vérifier le service.
7. Une fois le nom du service vérifié avec succès, choisissez le VPC où réside votre instance. Ajoutez la politique suivante pour limiter l'utilisation des points de terminaison Amazon VPC au compte spécifié uniquement. Avec l'organisation Condition indiquée sous cette stratégie, vous pouvez mettre à jour la stratégie suivante pour restreindre l'accès à votre point de terminaison. Pour fournir la prise en charge des points de terminaison Amazon VPC à des identifiants de compte spécifiques de votre organisation, consultez. [Organization condition to restrict access to your endpoint](#)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
  ],
}
```

```
{
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  },
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Principal": "*"
}
```

L'ID de compte `aws:PrincipalAccount` doit correspondre au compte contenant le VPC et le point de terminaison d'un VPC. La liste suivante indique comment partager le point de terminaison VPC avec d'autres identifiants de AWS compte :

- Pour spécifier plusieurs comptes pour accéder au point de terminaison VPC, remplacez-le `"aws:PrincipalAccount": "111122223333"` par le bloc suivant :

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
]
```

Assurez-vous de remplacer les identifiants de AWS compte par les identifiants de compte des comptes qui doivent accéder au point de terminaison du VPC.

- Pour autoriser tous les membres d'une organisation à accéder au point de terminaison VPC, remplacez-le `"aws:PrincipalAccount": "111122223333"` par la ligne suivante :

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

Assurez-vous de remplacer l'organisation ***o-abcdef0123*** par votre identifiant d'organisation.

- Pour restreindre l'accès à une ressource par un identifiant d'organisation, ajoutez votre `ResourceOrgID` nom à la politique. Pour plus d'informations, consultez [aws:ResourceOrgID](#) dans le Guide de l'utilisateur IAM.


```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Sous Paramètres supplémentaires, choisissez Activer le nom DNS.
9. Sous Sous-réseaux, choisissez les sous-réseaux dans lesquels réside votre instance.
10. Sous Groupes de sécurité, choisissez un groupe de sécurité dont le port entrant 443 est activé depuis votre VPC (ou votre instance Amazon EC2). Si vous ne possédez pas encore de groupe de sécurité dont le port entrant 443 est activé, consultez la section [Créer un groupe de sécurité pour votre VPC](#) dans le guide de l'utilisateur Amazon VPC.

En cas de problème lors de la restriction des autorisations entrantes sur votre VPC (ou instance), vous pouvez accéder au port 443 entrant depuis n'importe quelle adresse IP. (0.0.0.0/0)
Toutefois, il est GuardDuty recommandé d'utiliser des adresses IP correspondant au bloc CIDR de votre VPC. Pour plus d'informations, consultez la section [Blocs d'adresse CIDR VPC dans le guide](#) de l'utilisateur Amazon VPC.

Après avoir suivi les étapes, consultez [Validation de la configuration des points de terminaison VPC](#) pour vous assurer que le point de terminaison VPC a été correctement configuré.

Installation manuelle de l'agent de sécurité

GuardDuty fournit les deux méthodes suivantes pour installer l'agent GuardDuty de sécurité sur vos instances Amazon EC2. Avant de continuer, assurez-vous de suivre les étapes ci-dessous [Prérequis — Création manuelle d'un point de terminaison Amazon VPC](#).

Choisissez une méthode d'accès préférée pour installer l'agent de sécurité dans vos ressources Amazon EC2.

- [Méthode 1 - Utilisation AWS Systems Manager](#)— Cette méthode nécessite la gestion de votre instance Amazon EC2. AWS Systems Manager
- [Méthode 2 - Utilisation des gestionnaires de packages Linux](#)— Vous pouvez utiliser cette méthode, que vos instances Amazon EC2 soient AWS Systems Manager gérées ou non. En fonction des [distributions de votre système d'exploitation](#), vous pouvez choisir une méthode appropriée pour installer des scripts RPM ou des scripts Debian. Si vous utilisez la plateforme Fedora, vous devez utiliser cette méthode pour installer l'agent.

Méthode 1 - Utilisation AWS Systems Manager

Pour utiliser cette méthode, assurez-vous que vos instances Amazon EC2 sont AWS Systems Manager gérées, puis installez l'agent.

AWS Systems Manager instance Amazon EC2 gérée

Suivez les étapes ci-dessous pour gérer vos instances AWS Systems Manager Amazon EC2.

- [AWS Systems Manager](#) vous aide à gérer vos AWS applications et vos ressources de bout en bout et à sécuriser les opérations à grande échelle.

Pour gérer vos instances Amazon EC2 avec AWS Systems Manager, consultez la section [Configuration de Systems Manager pour les instances Amazon EC2](#) dans AWS Systems Manager le guide de l'utilisateur.

- Le tableau suivant présente les nouveaux AWS Systems Manager documents GuardDuty gérés :

Nom du document	Type de document	Objectif
AmazonGuardDuty-RunTimeMonitoringSsmPlugin	Distributeur	Pour emballer l'agent GuardDuty de sécurité.
AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin	Commande	Pour exécuter le script installation/un -installation afin d'installer l'agent GuardDuty de sécurité.

Pour plus d'informations AWS Systems Manager, consultez les documents [Amazon EC2 Systems Manager](#) dans AWS Systems Manager le guide de l'utilisateur.

Pour les serveurs Debian

Les Amazon Machine Images (AMI) pour le serveur Debian fournies par vous AWS obligent à installer l' AWS Systems Manager agent (agent SSM). Vous devrez effectuer une étape supplémentaire pour installer l'agent SSM afin que vos instances du serveur Amazon EC2 Debian soient gérées par SSM. Pour plus d'informations sur les étapes

à suivre, consultez la section [Installation manuelle de l'agent SSM sur les instances du serveur Debian](#) dans le guide de l'AWS Systems Manager utilisateur.

Pour installer l' GuardDuty agent pour l'instance Amazon EC2 en utilisant AWS Systems Manager

1. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
2. Dans le volet de navigation, sélectionnez Documents
3. Dans Owned by Amazon, sélectionnez AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
4. Choisissez Run Command (Exécuter une commande).
5. Entrez les paramètres d'exécution de la commande suivants
 - Action : Choisissez Installer.
 - Type d'installation : Choisissez Installer ou Désinstaller.
 - Nom : AmazonGuardDuty-RuntimeMonitoringSsmPlugin
 - Version : si ce champ reste vide, vous obtiendrez la dernière version de l'agent de GuardDuty sécurité. Pour plus d'informations sur les versions publiées, [GuardDuty versions de l'agent de sécurité pour les instances Amazon EC2](#).
6. Sélectionnez l'instance Amazon EC2 ciblée. Vous pouvez sélectionner une ou plusieurs instances Amazon EC2. Pour plus d'informations, voir [AWS Systems Manager Exécution de commandes depuis la console](#) dans le Guide de AWS Systems Manager l'utilisateur
7. Vérifiez si l'installation de l' GuardDuty agent est saine. Pour plus d'informations, consultez [Validation de l'état d'installation GuardDuty de l'agent de sécurité](#).

Méthode 2 - Utilisation des gestionnaires de packages Linux

Avec cette méthode, vous pouvez installer l'agent GuardDuty de sécurité en exécutant des scripts RPM ou des scripts Debian. En fonction des systèmes d'exploitation, vous pouvez choisir une méthode préférée :

- Utilisez des scripts RPM pour installer l'agent de sécurité sur les distributions du système d'exploitation AL2, AL2023 RedHat, CentOS ou Fedora.

- Utilisez des scripts Debian pour installer l'agent de sécurité sur les distributions du système d'exploitation Ubuntu ou Debian. Pour plus d'informations sur les distributions de systèmes d'exploitation Ubuntu et Debian prises en charge, consultez [Valider les exigences architecturales](#).

RPM installation

Important

Nous vous recommandons de vérifier la signature RPM de l'agent de GuardDuty sécurité avant de l'installer sur votre machine.

1. Vérifiez la signature RPM GuardDuty de l'agent de sécurité

a. Préparez le modèle

Préparez les commandes avec la clé publique appropriée, la signature du fichier x86_64 tr/min, la signature du fichier arm64 tr/min et le lien d'accès correspondant aux scripts RPM hébergés dans les compartiments Amazon S3. Remplacez la valeur du Région AWS, l'ID de AWS compte et la version de l' GuardDuty agent pour accéder aux scripts RPM.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/publickey.pem
```

- GuardDuty signature RPM de l'agent de sécurité :

Signature de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/x86_64/amazon-guardduty-agent-1.17.1.x86_64.sig
```

Signature d'arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/arm64/amazon-guardduty-agent-1.17.1.arm64.sig
```

- Liens d'accès aux scripts RPM du compartiment Amazon S3 :

Lien d'accès pour x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.rpm
```

Lien d'accès pour arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/arm64/
amazon-guardduty-agent-1.17.1.arm64.rpm
```

Région AWS	Nom de la région	AWS ID de compte
eu-west-1	Europe (Irlande)	694911143906
us-east-1	USA Est (Virginie du Nord)	593207742271
us-west-2	USA Ouest (Oregon)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	USA Est (Ohio)	307168627858
eu-central-1	Europe (Francfort)	323658145986
ap-northeast-2	Asie-Pacifique (Séoul)	914738172881
eu-north-1	Europe (Stockholm)	591436053604
ap-east-1	Asie-Pacifique (Hong Kong)	258348409381
me-south-1	Middle East (Bahrain)	536382113932
eu-west-2	Europe (Londres)	892757235363
ap-northeast-1	Asie-Pacifique (Tokyo)	533107202818

ap-southeast-1	Asie-Pacifique (Singapour)	174946120834
ap-south-1	Asie-Pacifique (Mumbai)	251508486986
ap-southeast-3	Asie-Pacifique (Jakarta)	510637619217
sa-east-1	Amérique du Sud (São Paulo)	758426053663
ap-northeast-3	Asie-Pacifique (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Afrique (Le Cap)	197869348890
ap-southeast-2	Asie-Pacifique (Sydney)	005257825471
me-central-1	Moyen-Orient (EAU)	000014521398
us-west-1	USA Ouest (Californie du Nord)	684579721401
ca-central-1	Canada (Centre)	354763396469
ca-west-1	Canada-Ouest (Calgary)	339712888787
ap-south-2	Asie-Pacifique (Hyderabad)	950823858135
eu-south-2	Europe (Espagne)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asie-Pacifique (Melbourne)	251357961535
ap-southeast-7	Asie-Pacifique (Thaïlande)	054037130133
il-central-1	Israël (Tel Aviv)	870907303882

mx-central-1	Mexique (Centre)	982081086614
ap-east-2	Asie-Pacifique (Taipei)	259886477082

b. Téléchargez le modèle

Dans la commande suivante, pour télécharger la clé publique appropriée, la signature du fichier x86_64 tr/min, la signature du fichier arm64 tr/min et le lien d'accès correspondant aux scripts RPM hébergés dans les compartiments Amazon S3, assurez-vous de remplacer l'ID de compte par l'identifiant approprié Compte AWS et la région par votre région actuelle.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.rpm ./amazon-guardduty-
agent-1.17.1.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.sig ./amazon-guardduty-
agent-1.17.1.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
publickey.pem ./publickey.pem
```

c. Importer la clé publique

Utilisez la commande suivante pour importer la clé publique dans la base de données :

```
gpg --import publickey.pem
```

gpg affiche l'importation avec succès

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Vérifiez la signature

Utilisez la commande suivante pour vérifier la signature

```
gpg --verify amazon-guardduty-agent-1.17.1.x86_64.sig amazon-guardduty-
agent-1.17.1.x86_64.rpm
```

Si la vérification est réussie, vous verrez un message similaire au résultat ci-dessous. Vous pouvez maintenant procéder à l'installation de l'agent de GuardDuty sécurité à l'aide de RPM.

Exemple de sortie :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
gpg:          owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Si la vérification échoue, cela signifie que la signature sur RPM a été potentiellement falsifiée. Vous devez supprimer la clé publique de la base de données et recommencer le processus de vérification.

Exemple :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Utilisez la commande suivante pour supprimer la clé publique de la base de données :

```
gpg --delete-keys AwsGuardDuty
```

Maintenant, réessayez le processus de vérification.

2. [Connectez-vous via SSH depuis Linux ou macOS.](#)
3. Installez l'agent GuardDuty de sécurité à l'aide de la commande suivante :

```
sudo rpm -ivh amazon-guardduty-agent-1.17.1.x86_64.rpm
```

4. Vérifiez si l'installation de l'agent GuardDuty est saine. Pour plus d'informations sur les étapes, consultez [Validation de l'état d'installation GuardDuty de l'agent de sécurité.](#)

Debian installation

Important

Nous recommandons de vérifier la signature GuardDuty de l'agent de sécurité Debian avant de l'installer sur votre machine.

1. Vérifier la signature GuardDuty de l'agent de sécurité Debian

- a. Préparez des modèles pour la clé publique appropriée, la signature du paquet Debian amd64, la signature du paquet Debian arm64 et le lien d'accès correspondant aux scripts Debian hébergés dans les compartiments Amazon S3

Dans les modèles suivants, remplacez la valeur du Région AWS, l'ID de AWS compte et la version de l' GuardDutyagent pour accéder aux scripts des paquets Debian.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/publickey.pem
```

- GuardDuty Signature de l'agent de sécurité Debian :

Signature d'amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/amd64/amazon-guardduty-agent-1.17.1.amd64.sig
```

Signature d'arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/arm64/amazon-guardduty-agent-1.17.1.arm64.sig
```

- Liens d'accès aux scripts Debian dans le compartiment Amazon S3 :

Lien d'accès pour amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/amd64/amazon-guardduty-agent-1.17.1.amd64.deb
```

Lien d'accès pour arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/arm64/
amazon-guardduty-agent-1.17.1.arm64.deb
```

Région AWS	Nom de la région	AWS ID de compte
eu-west-1	Europe (Irlande)	694911143906
us-east-1	USA Est (Virginie du Nord)	593207742271
us-west-2	USA Ouest (Oregon)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	USA Est (Ohio)	307168627858
eu-central-1	Europe (Francfort)	323658145986
ap-northeast-2	Asie-Pacifique (Séoul)	914738172881
eu-north-1	Europe (Stockholm)	591436053604
ap-east-1	Asie-Pacifique (Hong Kong)	258348409381
me-south-1	Middle East (Bahrain)	536382113932
eu-west-2	Europe (Londres)	892757235363
ap-northeast-1	Asie-Pacifique (Tokyo)	533107202818
ap-southeast-1	Asie-Pacifique (Singapour)	174946120834
ap-south-1	Asie-Pacifique (Mumbai)	251508486986
ap-southeast-3	Asie-Pacifique (Jakarta)	510637619217

sa-east-1	Amérique du Sud (São Paulo)	758426053663
ap-northeast-3	Asie-Pacifique (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Afrique (Le Cap)	197869348890
ap-southeast-2	Asie-Pacifique (Sydney)	005257825471
me-central-1	Moyen-Orient (EAU)	000014521398
us-west-1	USA Ouest (Californie du Nord)	684579721401
ca-central-1	Canada (Centre)	354763396469
ca-west-1	Canada-Ouest (Calgary)	339712888787
ap-south-2	Asie-Pacifique (Hyderabad)	950823858135
eu-south-2	Europe (Espagne)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asie-Pacifique (Melbourne)	251357961535
il-central-1	Israël (Tel Aviv)	870907303882
mx-central-1	Mexique (Centre)	982081086614
ap-east-2	Asie-Pacifique (Taipei)	259886477082

- b. Téléchargez la clé publique appropriée, la signature d'amd64, la signature d'arm64 et le lien d'accès correspondant aux scripts Debian hébergés dans des compartiments Amazon S3

Dans les commandes suivantes, remplacez l'identifiant du compte par l' Compte AWS identifiant approprié, et la région par votre région actuelle.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
amd64/amazon-guardduty-agent-1.17.1.amd64.deb ./amazon-guardduty-
agent-1.17.1.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
amd64/amazon-guardduty-agent-1.17.1.amd64.sig ./amazon-guardduty-
agent-1.17.1.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
publickey.pem ./publickey.pem
```

- c. Importer la clé publique dans la base de données

```
gpg --import publickey.pem
```

gpg affiche l'importation avec succès

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

- d. Vérifiez la signature

```
gpg --verify amazon-guardduty-agent-1.17.1.amd64.sig amazon-guardduty-
agent-1.17.1.amd64.deb
```

Après une vérification réussie, vous verrez un message similaire au résultat suivant :

Exemple de sortie :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
```

```
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Vous pouvez maintenant procéder à l'installation de l'agent GuardDuty de sécurité à l'aide de Debian.

Cependant, si la vérification échoue, cela signifie que la signature du paquet Debian a été potentiellement falsifiée.

Exemple :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D  
gpg: BAD signature from "AwsGuardDuty"
```

Utilisez la commande suivante pour supprimer la clé publique de la base de données :

```
gpg --delete-keys AwsGuardDuty
```

Maintenant, réessayez le processus de vérification.

2. [Connectez-vous via SSH depuis Linux ou macOS.](#)
3. Installez l'agent GuardDuty de sécurité à l'aide de la commande suivante :

```
sudo dpkg -i amazon-guardduty-agent-1.17.1.amd64.deb
```

4. Vérifiez si l'installation de l' GuardDuty agent est saine. Pour plus d'informations sur les étapes, consultez [Validation de l'état d'installation GuardDuty de l'agent de sécurité.](#)

Erreur de mémoire insuffisante

Si vous rencontrez une out-of-memory erreur lors de l'installation ou de la mise à jour manuelle de l'agent de GuardDuty sécurité pour Amazon EC2, consultez. [Résolution d'une erreur de mémoire insuffisante](#)

Validation de l'état d'installation GuardDuty de l'agent de sécurité

Après avoir effectué les étapes d'installation de l'agent GuardDuty de sécurité, suivez les étapes suivantes pour valider le statut de l'agent :

Pour vérifier si l'agent GuardDuty de sécurité est sain

1. [Connectez-vous via SSH depuis Linux ou macOS.](#)
2. Exécutez la commande suivante pour vérifier l'état de l'agent GuardDuty de sécurité :

```
sudo systemctl status amazon-guardduty-agent
```

Si vous souhaitez consulter les journaux d'installation de l'agent de sécurité, ils sont disponibles sous `/var/log/amzn-guardduty-agent/`.

Pour consulter les journaux, faites `sudo journalctl -u amazon-guardduty-agent`.

Mise à jour manuelle GuardDuty de l'agent de sécurité pour l'instance Amazon EC2

GuardDuty publie des mises à jour des versions de l'agent de sécurité. Lorsque vous gérez l'agent de sécurité manuellement, vous êtes responsable de le mettre à jour pour vos instances Amazon EC2. Pour plus d'informations sur les nouvelles versions des agents, consultez [GuardDuty versions publiées de l'agent de sécurité](#) la section dédiée aux instances Amazon EC2. Pour recevoir des notifications concernant la sortie d'une nouvelle version de l'agent, consultez [Abonnement aux annonces Amazon GuardDuty SNS](#).

Pour mettre à jour manuellement l'agent de sécurité pour l'instance Amazon EC2

Le processus de mise à jour de l'agent de sécurité est le même que celui d'installation de l'agent de sécurité. Selon la méthode que vous avez utilisée pour installer l'agent, vous pouvez effectuer les étapes décrites dans [Installation manuelle de l'agent de sécurité](#) les instances Amazon EC2.

Si vous utilisez la [méthode 1 - En utilisant AWS Systems Manager](#), vous pouvez mettre à jour l'agent de sécurité à l'aide de la commande Exécuter. Utilisez la version de l'agent vers laquelle vous souhaitez effectuer la mise à jour.

Si vous utilisez la [méthode 2 - En utilisant les gestionnaires de packages Linux](#), vous pouvez utiliser les scripts comme indiqué dans la [Installation manuelle de l'agent de sécurité](#) section. Les scripts incluent déjà la dernière version de l'agent. Pour plus d'informations sur les versions récemment publiées de l'agent, consultez [GuardDuty versions de l'agent de sécurité pour les instances Amazon EC2](#).

Après avoir mis à jour l'agent de sécurité, vous pouvez vérifier l'état de l'installation en consultant les journaux. Pour plus d'informations, consultez [Validation de l'état d'installation GuardDuty de l'agent de sécurité](#).

Gestion GuardDuty de l'agent de sécurité sur Bottlerocket (Amazon ECS sur Amazon EC2)

Important

Cette page s'applique uniquement aux versions Bottlerocket ECS-optimized AMI v1.62.1 et ultérieures, y compris les variantes suivantes :

- `bottlerocket-aws-ecs-2-x86_64 / bottlerocket-aws-ecs-2-aarch64`
- `bottlerocket-aws-ecs-3-x86_64 / bottlerocket-aws-ecs-3-aarch64`
- `bottlerocket-aws-ecs-2-nvidia / bottlerocket-aws-ecs-2-nvidia-fips`
- `bottlerocket-aws-ecs-3-nvidia / bottlerocket-aws-ecs-3-nvidia-fips`

Pour les instances Bottlerocket dans les clusters Amazon EKS, Runtime Monitoring utilise une configuration différente. Consultez [Conditions préalables à la prise en charge des clusters Amazon EKS](#).

Cette page explique comment l'agent de GuardDuty sécurité s'exécute sur les ECS-optimized AMI Bottlerocket et comment GuardDuty il est déployé. Sur Bottlerocket, l'agent s'exécute en tant que conteneur hôte plutôt qu'en tant que paquet RPM ou Debian installé. Bottlerocket est un système d'exploitation Linux optimisé pour les conteneurs avec un système de fichiers racine immuable. Il n'utilise donc pas les gestionnaires de paquets traditionnels. GuardDuty héberge l'image du conteneur de l'agent dans un référentiel Amazon Elastic Container Registry (Amazon ECR) qu'il gère, et lorsque vous activez la surveillance du temps d'exécution avec une configuration automatique de l'agent GuardDuty, AWS Systems Manager utilise Distributor pour déployer le conteneur hôte de l'agent pour vous.

Conditions préalables

Avant de continuer, assurez-vous de suivre toutes les [Conditions préalables au support de ECS-EC2 Bottlerocket](#).

Activation de la configuration automatique des agents

Les ECS-EC2 instances Bottlerocket utilisent le même document SSM et la même configuration d'agent automatisée que les instances Amazon EC2 standard. Pour activer l'agent GuardDuty automatisé pour vos instances Bottlerocket, suivez les étapes décrites dans [Agent automatisé sur la ressource Amazon EC2](#). Cela inclut notamment les éléments suivants :

- GuardDuty Agent d'activation dans un environnement multi-comptes.
- Activation de l'agent GuardDuty automatisé dans un compte autonome.

Pour connaître les conditions supplémentaires requises lors de l'utilisation de balises d'inclusion ou d'exclusion, consultez [Lors de l'utilisation de la configuration automatique des agents](#).

Vérification de l'agent

Après avoir activé la configuration automatique de l'agent, vérifiez que l'agent est en cours d'exécution sur votre instance Bottlerocket :

1. Connectez-vous à votre instance à l'aide du gestionnaire de session SSM.
2. Entrez dans le conteneur d'administration : `enter-admin-container`.
3. Consultez les journaux des agents à l'aide de l'une des méthodes suivantes :
 - `sheltie journalctl -u host-containers@amazon-guardduty-agent`
 - À partir d'une session Sheltie (`sudo sheltie`) : `ls /var/log/amzn-guardduty-agent/`.

Pour plus d'informations sur l'examen des statistiques de couverture pour vos instances Amazon EC2, consultez [Consultation des statistiques de couverture](#).

Si l'état de couverture apparaît comme étant insalubre, consultez [Résolution des problèmes de couverture d'exécution de Bottlerocket ECS-EC2](#).

Gestion de l'agent de sécurité automatisé pour Fargate (Amazon ECS uniquement)

Runtime Monitoring prend en charge la gestion de l'agent de sécurité pour vos clusters Amazon ECS (AWS Fargate) uniquement via GuardDuty. La gestion manuelle de l'agent de sécurité sur les clusters Amazon ECS n'est pas prise en charge.

Avant de suivre les étapes décrites dans cette section, assurez-vous de les suivre [Prérequis pour AWS Fargate \(Amazon ECS uniquement\) support](#).

Sur la base des approches décrites dans [Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate](#), choisissez une méthode préférée pour activer l'agent GuardDuty automatisé pour vos ressources.

GuardDuty Agent de configuration pour un environnement multi-comptes

Dans un environnement à comptes multiples, seul le compte d'administrateur délégué GuardDuty peut activer ou désactiver la configuration automatique des agents pour les comptes membres, et gérer la configuration automatique des agents pour les clusters Amazon ECS appartenant aux comptes membres de leur organisation. Un compte GuardDuty membre ne peut pas modifier cette configuration. Le compte d'administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements multicomptes, consultez [la section Gestion de plusieurs comptes dans GuardDuty](#).

Activation de la configuration automatique des agents pour le compte GuardDuty d'administrateur délégué

Manage for all Amazon ECS clusters (account level)

Si vous avez choisi Activer pour tous les comptes pour la surveillance du temps d'exécution, les options suivantes s'offrent à vous :

- Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gèrera l'agent de sécurité pour toutes les tâches Amazon ECS lancées.
- Choisissez Configurer les comptes manuellement.

Si vous avez choisi Configurer les comptes manuellement dans la section Surveillance du temps d'exécution, procédez comme suit :

1. Choisissez Configurer les comptes manuellement dans la section Configuration automatique de l'agent.
2. Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).

Cliquez sur Enregistrer.

Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS avec la paire clé-valeur sous GuardDutyManaged la forme -. false
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
```

```

        "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],

```

```
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
```

3. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
4. Dans le volet de navigation, choisissez Runtime Monitoring.
- 5.

 Note

Ajoutez toujours la balise d'exclusion à vos clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

Dans l'onglet Configuration, choisissez Activer dans la configuration de l'agent automatisé.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

6. Cliquez sur Enregistrer.
7. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.

- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un cluster Amazon ECS pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être GuardDutyManaged -. true
2. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
```

```

        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

 Note

Lorsque vous utilisez des balises d'inclusion pour vos clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement GuardDuty l'agent via la configuration automatique de l'agent.

3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Auto-enable pour tous les comptes membres

Manage for all Amazon ECS clusters (account level)

Les étapes suivantes supposent que vous avez choisi Activer pour tous les comptes dans la section Runtime Monitoring.

1. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gèrera l'agent de sécurité pour toutes les tâches Amazon ECS lancées.
2. Cliquez sur Enregistrer.
3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS avec la paire clé-valeur sous GuardDutyManaged la forme -. false
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```



```

    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
}

```

```
}  
  }  
    }  
      ]  
        }
```

3. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
4. Dans le volet de navigation, choisissez Runtime Monitoring.
- 5.

 Note

Ajoutez toujours la balise d'exclusion à vos clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

Dans l'onglet Configuration, choisissez Modifier.

6. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gèrera le déploiement de l'agent de sécurité dans le conteneur annexe.

7. Cliquez sur Enregistrer.
8. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Quelle que soit la manière dont vous choisissez d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certaines tâches Amazon ECS Fargate pour tous les comptes membres de votre organisation.

1. N'activez aucune configuration dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle que vous avez sélectionnée à l'étape précédente.
2. Cliquez sur Enregistrer.
3. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ],
}
```

```

    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }

```

```
]
}
```

 Note

Lorsque vous utilisez des balises d'inclusion pour vos clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la gestion automatique des GuardDuty agents.

4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Activation de la configuration automatique des agents pour les comptes de membres actifs existants

Manage for all Amazon ECS clusters (account level)

1. Sur la page Runtime Monitoring, sous l'onglet Configuration, vous pouvez consulter l'état actuel de la configuration automatique des agents.
2. Dans le volet Configuration automatique de l'agent, dans la section Comptes membres actifs, sélectionnez Actions.
3. Dans Actions, choisissez Activer pour tous les comptes membres actifs existants.
4. Choisissez Confirmer.
5. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que

vous n'activez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS avec la paire clé-valeur sous GuardDutyManaged la forme -. false
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        }
      }
    }
  ]
}
```

```

        "Null": {
            "ecs:ResourceTag/GuardDutyManaged": false
        }
    },
    {
        "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            }
        }
    }
}

```

```
    "Null": {  
      "aws:PrincipalTag/GuardDutyManaged": true  
    }  
  }  
]  
}
```

3. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
4. Dans le volet de navigation, choisissez Runtime Monitoring.
- 5.

 Note

Ajoutez toujours la balise d'exclusion à vos clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

Sous l'onglet Configuration, dans la section Configuration automatique de l'agent, sous Comptes membres actifs, sélectionnez Actions.

6. Dans Actions, choisissez Activer pour tous les comptes membres actifs.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gèrera le déploiement de l'agent de sécurité dans le conteneur annexe.

7. Choisissez Confirmer.
8. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un cluster Amazon ECS pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être GuardDutyManaged -. true
2. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
    }
  ]
}
```

```

        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
]
}

```

 Note

Lorsque vous utilisez des balises d'inclusion pour vos clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Auto-enable Configuration automatique des agents pour les nouveaux membres

Manage for all Amazon ECS clusters (account level)

1. Sur la page Runtime Monitoring, choisissez Modifier pour mettre à jour la configuration existante.
2. Dans la section Configuration automatique de l'agent, sélectionnez Activer automatiquement pour les nouveaux comptes membres.
3. Cliquez sur Enregistrer.
4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS avec la paire clé-valeur sous GuardDutyManaged la forme -. false
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }
}

```

```
}  
]  
}
```

3. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
4. Dans le volet de navigation, choisissez Runtime Monitoring.

5.

 Note

Ajoutez toujours la balise d'exclusion à vos clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

Dans l'onglet Configuration, sélectionnez Activer automatiquement pour les nouveaux comptes membres dans la section Configuration automatique des agents.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gèrera le déploiement de l'agent de sécurité dans le conteneur annexe.

6. Cliquez sur Enregistrer.
7. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un cluster Amazon ECS pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged -. true`

2. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
```

```

        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
]
}

```

 Note

Lorsque vous utilisez des balises d'inclusion pour vos clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Activation sélective de la configuration automatique des agents pour les comptes de membres actifs

Manage for all Amazon ECS (account level)

1. Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration de Monitoring-Automated l'agent Runtime (ECS-Fargate). Vous pouvez sélectionner plusieurs comptes. Assurez-vous que les comptes que vous sélectionnez à cette étape sont déjà activés avec Runtime Monitoring.
2. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration de Monitoring-Automated l'agent Runtime (ECS-Fargate).
3. Choisissez Confirmer.
4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS avec la paire clé-valeur sous GuardDutyManaged la forme -. false
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
```

```

    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

3. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
4. Dans le volet de navigation, choisissez Runtime Monitoring.

5.

 Note

Ajoutez toujours la balise d'exclusion à vos clusters Amazon ECS avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration de Monitoring-Automated l'agent Runtime (ECS-Fargate). Vous pouvez sélectionner plusieurs comptes. Assurez-vous que les comptes que vous sélectionnez à cette étape sont déjà activés avec Runtime Monitoring.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

6. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration de Monitoring-Automated l'agent Runtime (ECS-Fargate).
7. Cliquez sur Enregistrer.
8. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Assurez-vous de ne pas activer la configuration automatique de l'agent (ou la configuration de l' Monitoring-Automated agent d'exécution (ECS-Fargate)) pour les comptes sélectionnés dotés des clusters Amazon ECS que vous souhaitez surveiller.

2. Ajoutez une balise à un cluster Amazon ECS pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être GuardDutyManaged -. true
3. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

 Note

Lorsque vous utilisez des balises d'inclusion pour vos clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Configuration de GuardDuty l'agent pour un compte autonome

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sous l'onglet Configuration :
 - a. Pour gérer la configuration automatisée des agents pour tous les clusters Amazon ECS (au niveau du compte)

Choisissez Activer dans la section Configuration automatique de l'agent pour AWS Fargate (ECS uniquement). Lorsqu'une nouvelle tâche Fargate Amazon ECS est GuardDuty lancée, il gère le déploiement de l'agent de sécurité.

- Cliquez sur Enregistrer.

- b. Pour gérer la configuration automatisée des agents en excluant certains clusters Amazon ECS (au niveau du cluster)
 - i. Ajoutez une balise au cluster Amazon ECS pour lequel vous souhaitez exclure toutes les tâches. La paire clé-valeur doit être GuardDutyManaged -. false
 - ii. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn":
            "arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
```



```

        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

- iii. Sous l'onglet Configuration, choisissez Activer dans la section Configuration automatique de l'agent.

 Note

Ajoutez toujours la balise d'exclusion à votre cluster Amazon ECS avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de sécurité sera déployé dans toutes les tâches lancées au sein du cluster Amazon ECS correspondant.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

- iv. Cliquez sur Enregistrer.
- c. Pour gérer la configuration automatisée des agents en incluant certains clusters Amazon ECS (au niveau du cluster)
 - i. Ajoutez une balise à un cluster Amazon ECS pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être GuardDutyManaged -. true
 - ii. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans [Empêcher la modification des balises, sauf selon les principes autorisés](#) dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
```

```

        "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],

```

```
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn":
                    "arn:aws:iam::123456789012:role/org-admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
}
```

4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un service ECS spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant `forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- [Mettre à jour un service Amazon ECS à l'aide de la console décrite](#) dans le manuel Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) dans le manuel Amazon Elastic Container Service API Reference.
- [update-service dans le manuel](#) de référence des AWS CLI commandes.

Gestion automatique de l'agent de sécurité pour les ressources Amazon EKS

La surveillance du temps d'exécution prend en charge l'activation de l'agent de sécurité par le biais d'une configuration GuardDuty automatique et manuelle. Cette section décrit les étapes permettant d'activer la configuration automatique des agents pour les clusters Amazon EKS.

Avant de continuer, assurez-vous d'avoir suivi le [Conditions préalables à la prise en charge des clusters Amazon EKS](#).

En fonction de l'approche que vous préférez [Configuration automatique de l'agent \(recommandée\)](#), choisissez les étapes correspondantes dans les sections suivantes.

Configuration de l'agent automatisé pour les environnements multi-comptes

Dans les environnements à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la configuration automatique des agents pour les comptes des membres et gérer l'agent automatique pour les clusters EKS appartenant aux comptes membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter [Managing multiple accounts](#).

Configuration de la configuration automatique de l'agent pour le compte GuardDuty administrateur délégué

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveiller tous les clusters EKS)	<p>Si vous avez choisi Activer pour tous les comptes dans la section Surveillance du temps d'exécution, les options suivantes s'offrent à vous :</p> <ul style="list-style-type: none">• Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gérera l'agent de sécurité pour tous les clusters EKS appartenant au compte de compte d' GuardDuty administrateur délégué ainsi que pour tous les clusters EKS appartenant à tous les comptes membres existants et potentiellement nouveaux de l'organisation.• Choisissez Configurer les comptes manuellement. <p>Si vous avez choisi Configurer les comptes manuellement dans la section Surveillance du temps d'exécution, procédez comme suit :</p> <ol style="list-style-type: none">1. Choisissez Configurer les comptes manuellement dans la section Configuration automatique de l'agent.2. Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).

Approche préférée
pour gérer les agents
GuardDuty de sécurité

Étapes

Cliquez sur Enregistrer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)	<p>Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.</p> <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster</p> <ol style="list-style-type: none"> 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <ol style="list-style-type: none"> 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> . • Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> . • Remplacez <code>123456789012</code> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ol style="list-style-type: none"> Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/. Dans le volet de navigation, choisissez Runtime Monitoring. <div data-bbox="586 489 1507 850" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> </div> <ol style="list-style-type: none"> Dans l'onglet Configuration, choisissez Activer dans la section de gestion des GuardDuty agents. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gèrera le déploiement et les mises à jour de l'agent GuardDuty de sécurité. Cliquez sur Enregistrer. <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster</p> <ol style="list-style-type: none"> Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :</p> <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . • Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . • Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3. Si vous avez activé l'agent automatique pour ce cluster EKS, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce cluster EKS. Cela peut avoir un impact sur vos statistiques d'utilisation.</p> <p>Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.</p> <p>4. Si vous gérez manuellement l'agent de GuardDuty sécurité pour ce cluster EKS, consultez Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS sélectifs à l'aide de balises d'inclusion	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certains clusters EKS de votre compte :</p> <ol style="list-style-type: none"> 1. Assurez-vous de choisir Désactiver pour le compte GuardDuty administrateur délégué (ce compte) dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Cliquez sur Enregistrer. 3. Ajoutez une balise à votre cluster EKS avec la clé en tant que GuardDutyManaged et sa valeur en tant que true. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés que vous souhaitez surveiller.</p> <ol style="list-style-type: none"> 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . • Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . • Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	<p>Étapes</p> <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Gestion manuelle de l'agent de GuardDuty sécurité	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, vous pouvez gérer l'agent de sécurité manuellement pour vos clusters EKS.</p> <ol style="list-style-type: none">1. Assurez-vous de choisir Désactiver pour le compte GuardDuty administrateur délégué (ce compte) dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente.2. Cliquez sur Enregistrer.3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Auto-enable Agent automatisé pour tous les comptes des membres

Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Gérez l'agent de sécurité via GuardDuty</p> <p>(Surveiller tous les clusters EKS)</p>	<p>Cette rubrique vise à activer la surveillance du temps d'exécution pour tous les comptes membres. Par conséquent, les étapes suivantes supposent que vous devez avoir choisi Activer pour tous les comptes dans la section Surveillance du temps d'exécution.</p> <ol style="list-style-type: none"> 1. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gèrera l'agent de sécurité pour tous les clusters EKS appartenant au compte de compte d' GuardDuty administrateur délégué ainsi que pour tous les clusters EKS appartenant à tous les comptes membres existants et potentiellement nouveaux de l'organisation. 2. Cliquez sur Enregistrer.
<p>Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)</p>	<p>Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.</p> <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster</p> <ol style="list-style-type: none"> 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <ol style="list-style-type: none"> 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> .• Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> .• Remplacez <i>123456789012</i> par l' ID Compte AWS de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.4. Dans le volet de navigation, choisissez Runtime Monitoring. <div> Note<p>Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer l'agent automatisé pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p></div> <ol style="list-style-type: none">5. Sous l'onglet Configuration, choisissez Modifier dans la section Configuration de la surveillance du temps d'exécution.6. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gèrera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.7. Cliquez sur Enregistrer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster</p> <ol style="list-style-type: none"> 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 2. Si la configuration automatique de l'agent est activée pour ce cluster EKS, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce cluster EKS. Cela peut avoir un impact sur vos statistiques d'utilisation. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring. 3. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> . • Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez 123456789012 par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">4. Si vous gérez manuellement l'agent de GuardDuty sécurité pour ce cluster EKS, consultez Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS sélectifs à l'aide de balises d'inclusion	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certains clusters EKS pour tous les comptes membres de votre organisation :</p> <ol style="list-style-type: none"> 1. N'activez aucune configuration dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Cliquez sur Enregistrer. 3. Ajoutez une balise à votre cluster EKS avec la clé en tant que GuardDutyManaged et sa valeur en tant que true. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés que vous souhaitez surveiller.</p> <ol style="list-style-type: none"> 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . • Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . • Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance.

<p>Approche préférée pour gérer les agents GuardDuty de sécurité</p>	<p>Étapes</p>
	<p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
<p>Gestion manuelle de l'agent de GuardDuty sécurité</p>	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, vous pouvez gérer l'agent de sécurité manuellement pour vos clusters EKS.</p> <ol style="list-style-type: none"> 1. N'activez aucune configuration dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Cliquez sur Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Activation de l'agent automatique pour tous les comptes de membres actifs existants

Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Pour gérer l'agent GuardDuty de sécurité pour les comptes de membres actifs existants de votre organisation

- **GuardDuty** Pour recevoir les événements d'exécution des clusters EKS appartenant aux comptes de membres actifs existants de l'organisation, vous devez choisir une approche préférée pour gérer l'agent de GuardDuty sécurité pour ces clusters EKS. Pour plus

d'informations sur ces approches, veuillez consulter [Déploiement de l'agent de sécurité sur Amazon EKS](#).

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveiller tous les clusters EKS)	<p>Pour surveiller tous les clusters EKS pour tous les comptes membres actifs existants</p> <ol style="list-style-type: none">1. Sur la page Runtime Monitoring, sous l'onglet Configuration, vous pouvez consulter l'état actuel de la configuration automatique des agents.2. Dans le volet Configuration automatique de l'agent, dans la section Comptes membres actifs, sélectionnez Actions.3. Dans Actions, choisissez Activer pour tous les comptes membres actifs existants.4. Choisissez Confirmer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)</p>	<p>Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.</p> <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster</p> <ol style="list-style-type: none">1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <ol style="list-style-type: none">2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none">• Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> .• Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> .• Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> .• Remplacez <code>123456789012</code> par l' ID de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre data-bbox="803 449 1396 678">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="691 720 1442 804">3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.<li data-bbox="691 825 1430 909">4. Dans le volet de navigation, choisissez Runtime Monitoring. <div data-bbox="784 984 820 1024"></div> <div data-bbox="829 984 904 1018">Note</div> <p data-bbox="829 1043 1458 1318">Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> <ol style="list-style-type: none"><li data-bbox="691 1375 1502 1507">5. Sous l'onglet Configuration, dans le volet Configuration automatique de l'agent, sous Comptes membres actifs, sélectionnez Actions.<li data-bbox="691 1528 1406 1612">6. Dans Actions, choisissez Activer pour tous les comptes membres actifs.<li data-bbox="691 1633 1065 1667">7. Choisissez Confirmer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Pour exclure un cluster EKS de la surveillance une fois que l'agent de GuardDuty sécurité a déjà été déployé sur ce cluster</p> <ol style="list-style-type: none">1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). Après cette étape, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce cluster EKS. Cela peut avoir un impact sur vos statistiques d'utilisation.2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :<ul style="list-style-type: none">• Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> .• Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> .• Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez 123456789012 par l' ID du compte AWS de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. Quelle que soit la façon dont vous gérez l'agent de sécurité (par le biais GuardDuty ou manuellement), pour ne plus recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller des clusters EKS sélectifs à l'aide de balises d'inclusion</p>	<ol style="list-style-type: none"> 1. Sur la page Comptes, une fois que vous avez activé la surveillance du temps d'exécution, n'activez pas la surveillance du temps d'exécution - Configuration automatique de l'agent. 2. Ajoutez une balise au cluster EKS qui appartient au compte sélectionné que vous souhaitez surveiller. La paire clé-valeur de la balise doit être GuardDuty Managed -true. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés que vous souhaitez surveiller.</p> 3. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDuty Managed . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Gestion manuelle de l'agent de GuardDuty sécurité	<ol style="list-style-type: none"> 1. Assurez-vous de ne pas sélectionner Activer dans la section Configuration automatique de l'agent. Maintenez la surveillance du temps d'exécution activée. 2. Cliquez sur Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Auto-enable configuration automatique des agents pour les nouveaux membres

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Gérez l'agent de sécurité via GuardDuty</p> <p>(Surveiller tous les clusters EKS)</p>	<ol style="list-style-type: none"> 1. Sur la page Runtime Monitoring, choisissez Modifier pour mettre à jour la configuration existante. 2. Dans la section Configuration automatique de l'agent, sélectionnez Activer automatiquement pour les nouveaux comptes membres. 3. Cliquez sur Enregistrer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)</p>	<p>Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.</p> <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster</p> <ol style="list-style-type: none">1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <ol style="list-style-type: none">2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none">• Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> .• Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> .• Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> .• Remplacez <code>123456789012</code> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<div data-bbox="747 262 1507 493"><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></div> <ol style="list-style-type: none"><li data-bbox="654 510 1401 594">3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.<li data-bbox="654 615 1390 699">4. Dans le volet de navigation, choisissez Runtime Monitoring. <div data-bbox="714 741 1507 1150"><p> Note</p><p>Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p></div> <ol style="list-style-type: none"><li data-bbox="654 1167 1482 1472">5. Dans l'onglet Configuration, sélectionnez Activer automatiquement les nouveaux comptes membres dans la section Gestion des GuardDuty agents. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gèrera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.<li data-bbox="654 1493 1047 1535">6. Cliquez sur Enregistrer. <p data-bbox="654 1602 1471 1686">Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster</p> <ol style="list-style-type: none"><li data-bbox="654 1728 1498 1812">1. Que vous gériez l'agent GuardDuty de sécurité par le biais GuardDuty ou manuellement, ajoutez une balise à

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>ce cluster EKS avec la clé <code>GuardDutyManaged</code> et sa valeur <code>asfalse</code>.</p> <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>Si l'agent automatisé est activé pour ce cluster EKS, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce cluster EKS. Cela peut avoir un impact sur vos statistiques d'utilisation.</p> <p>Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.</p> <ol style="list-style-type: none"> 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez <i>access-project</i> par GuardDuty Managed .• Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. Si vous gérez manuellement l'agent de GuardDuty sécurité pour ce cluster EKS, consultez Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller des clusters EKS sélectifs à l'aide de balises d'inclusion</p>	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certains clusters EKS pour les nouveaux comptes membres de votre organisation.</p> <ol style="list-style-type: none">1. Assurez-vous de désactiver l'option Activer automatiquement pour les nouveaux comptes membres dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente.2. Cliquez sur Enregistrer.3. Ajoutez une balise à votre cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>true</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés que vous souhaitez surveiller.</p> <ol style="list-style-type: none">4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none">• Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez <i>ec2:DeleteTags</i> par <i>eks:UntagResource</i> .• Remplacez <i>access-project</i> par <i>GuardDutyManaged</i> .• Remplacez <i>123456789012</i> par l' ID Compte AWS de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Gestion manuelle de l'agent de GuardDuty sécurité	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, vous pouvez gérer l'agent de sécurité manuellement pour vos clusters EKS.</p> <ol style="list-style-type: none">1. Assurez-vous de décocher la case Activer automatiquement pour les nouveaux comptes membres dans la section Configuration automatique des agents. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente.2. Cliquez sur Enregistrer.3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Configuration sélective de l'agent automatisé pour les comptes de membres actifs

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Gérez l'agent de sécurité via GuardDuty</p> <p>(Surveiller tous les clusters EKS)</p>	<ol style="list-style-type: none"> 1. Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration automatique des agents. Vous pouvez sélectionner plusieurs comptes à la fois. Assurez-vous que la surveillance d'exécution EKS est déjà activée sur les comptes que vous sélectionnez au cours de cette étape. 2. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer Runtime Monitoring - Configuration automatisée des agents. 3. Choisissez Confirmer.
<p>Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)</p>	<p>Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.</p> <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster</p> <ol style="list-style-type: none"> 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <ol style="list-style-type: none"> 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez <i>access-project</i> par GuardDutyManaged .• Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/. <div> Note<p>Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p></div> <ol style="list-style-type: none">4. Sur la page Comptes, sélectionnez le compte pour lequel vous souhaitez activer Gérer automatiquement l'agent. Vous pouvez sélectionner plusieurs comptes à la fois.5. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration de Monitoring-Automated l'agent Runtime pour le compte sélectionné. <p>Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.</p> <ol style="list-style-type: none">6. Cliquez sur Enregistrer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster</p> <ol style="list-style-type: none"> 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>false</code>. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). <p>Si la configuration automatique de l'agent était précédemment activée pour ce cluster EKS, l'agent de sécurité de ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce cluster EKS. Cela peut avoir un impact sur vos statistiques d'utilisation.</p> <p>Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.</p> 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> . • Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez 123456789012 par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <div data-bbox="618 554 1507 751"><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></div> <ol style="list-style-type: none">3. Si vous gérez manuellement l'agent de GuardDuty sécurité pour ce cluster EKS, vous devez le supprimer. Pour plus d'informations, consultez Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller des clusters EKS sélectifs à l'aide de balises d'inclusion</p>	<p>Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certains clusters EKS appartenant aux comptes sélectionnés :</p> <ol style="list-style-type: none"> 1. Assurez-vous de ne pas activer la configuration de Monitoring-Automated l'agent Runtime pour les comptes sélectionnés dotés des clusters EKS que vous souhaitez surveiller. 2. Ajoutez une balise à votre cluster EKS avec la clé en tant que <code>GuardDutyManaged</code> et sa valeur en tant que <code>true</code>. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>Après avoir ajouté la balise, GuardDuty il gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectifs que vous souhaitez surveiller.</p> <ol style="list-style-type: none"> 3. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> . • Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> . • Remplacez <code>123456789012</code> par l' ID Compte AWS de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<pre data-bbox="639 323 1406 478">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Gestion manuelle de l'agent de GuardDuty sécurité	<ol style="list-style-type: none"> 1. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. Assurez-vous de ne pas activer Runtime Monitoring - Configuration automatique de l'agent pour aucun des comptes sélectionnés. 2. Choisissez Confirmer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Configuration de l'agent automatisé pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour plus d'informations, consultez [Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples](#).

Après avoir activé la surveillance du temps d'exécution, veuillez à installer l'agent GuardDuty de sécurité par le biais d'une configuration automatique ou d'un déploiement manuel. Dans le cadre de toutes les étapes répertoriées dans la procédure suivante, veuillez à installer l'agent de sécurité.

Selon votre préférence en matière de surveillance de toutes les ressources Amazon EKS ou de certaines d'entre elles, choisissez une méthode préférée et suivez les étapes décrites dans le tableau suivant.

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Dans l'onglet Configuration, choisissez Activer pour activer la configuration automatique des agents pour votre compte.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveiller tous les clusters EKS)	<ol style="list-style-type: none"> 1. Choisissez Activer dans la section Configuration automatique de l'agent. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters EKS existants et potentiellement nouveaux de votre compte. 2. Cliquez sur Enregistrer.
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<p>Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.</p> <p>Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster</p> <ol style="list-style-type: none"> 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que GuardDutyManaged et sa valeur en tant que false. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <ol style="list-style-type: none"> 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez <i>ec2:CreateTags</i> par <i>eks:TagResource</i> .• Remplacez <i>ec2:DeleteTags</i> par <i>eks:UntagResource</i> .• Remplacez <i>access-project</i> par <i>GuardDutyManaged</i> .• Remplacez <i>123456789012</i> par l' ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.4. Dans le volet de navigation, choisissez Runtime Monitoring. <div> Note<p>Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p></div>

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	<ol style="list-style-type: none"><li data-bbox="690 260 1498 342">5. Dans l'onglet Configuration, choisissez Activer dans la section de gestion des GuardDuty agents. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.<li data-bbox="690 537 1089 573">6. Cliquez sur Enregistrer. Pour exclure un cluster EKS de la surveillance une fois que l'agent de GuardDuty sécurité a déjà été déployé sur ce cluster <ol style="list-style-type: none"><li data-bbox="690 825 1487 953">1. Ajoutez une balise à ce cluster EKS avec la clé en tant que GuardDutyManaged et sa valeur en tant que false. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). Après cette étape, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce cluster EKS. Cela peut avoir un impact sur vos statistiques d'utilisation.<li data-bbox="690 1566 1503 1833">2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	<ul style="list-style-type: none">• Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> .• Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> .• Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> .• Remplacez <i>123456789012</i> par l' ID du compte AWS de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
<p>Surveiller des clusters EKS sélectifs à l'aide de balises d'inclusion</p>	<ol style="list-style-type: none"> 1. Assurez-vous de choisir Désactiver dans la section Configuration automatique de l'agent. Maintenez la surveillance du temps d'exécution activée. 2. Choisissez Enregistrer. 3. Ajoutez une balise à ce cluster EKS avec la clé en tant que GuardDutyManaged et sa valeur en tant que true. <p>Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie).</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés que vous souhaitez surveiller.</p> 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDutyManaged . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	<p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre data-bbox="803 451 1396 682">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Gestion manuelle de l'agent	<ol style="list-style-type: none"> 1. Assurez-vous de choisir Désactiver dans la section Configuration automatique de l'agent. Maintenez la surveillance du temps d'exécution activée. 2. Cliquez sur Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS

Cette section décrit comment vous pouvez gérer votre agent complémentaire Amazon EKS (GuardDuty agent) après avoir activé Runtime Monitoring (ou EKS Runtime Monitoring). Pour utiliser Runtime Monitoring, vous devez activer Runtime Monitoring et configurer le module complémentaire Amazon EKS, `aws-guardduty-agent`. Vous devez effectuer les deux étapes pour GuardDuty détecter les menaces potentielles et générer [GuardDuty Types de recherche liés à la surveillance du temps](#).

Pour gérer l'agent manuellement, vous devez créer un point de terminaison VPC comme condition préalable. Cela permet de GuardDuty recevoir les événements d'exécution. Ensuite, vous pouvez installer l'agent de sécurité afin qu'il commence à GuardDuty recevoir les événements d'exécution provenant des ressources Amazon EKS. Lorsque vous GuardDuty publiez une nouvelle version d'agent pour cette ressource, vous pouvez mettre à jour la version de l'agent dans votre compte.

Rubriques

- [Prérequis — Création d'un point de terminaison Amazon VPC](#)
- [Installation manuelle GuardDuty de l'agent de sécurité sur les ressources Amazon EKS](#)
- [Mise à jour manuelle de l'agent de sécurité pour les ressources Amazon EKS](#)

Prérequis — Création d'un point de terminaison Amazon VPC

Avant de pouvoir installer l'agent GuardDuty de sécurité, vous devez créer un point de terminaison Amazon Virtual Private Cloud (Amazon VPC). Cela vous aidera à GuardDuty recevoir les événements d'exécution de vos ressources Amazon EKS.

Note

L'utilisation du point de terminaison VPC n'entraîne aucun coût supplémentaire.

Choisissez une méthode d'accès préférée pour créer un point de terminaison Amazon VPC.

Console

Pour créer un point de terminaison VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, sous Cloud privé virtuel, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Sur la page Créer un point de terminaison, pour Catégorie de services, choisissez Autres services de points de terminaison.
5. Pour Nom du service, entrez **com.amazonaws.us-east-1.guardduty-data**.

Assurez-vous de le remplacer **us-east-1** par la bonne région. Il doit s'agir de la même région que le cluster EKS qui appartient à votre Compte AWS identifiant.

6. Choisissez Vérifier le service.
7. Une fois le nom du service vérifié, choisissez le VPC dans lequel réside votre cluster. Ajoutez la stratégie suivante pour limiter l'utilisation de point de terminaison d'un VPC au compte spécifié uniquement. Avec l'organisation Condition indiquée sous cette stratégie, vous pouvez mettre à jour la stratégie suivante pour restreindre l'accès à votre point de terminaison. Pour fournir une prise en charge des points de terminaison d'un VPC à des

identifiants de compte spécifiques de votre organisation, veuillez consulter [Organization condition to restrict access to your endpoint](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

L'ID de compte `aws:PrincipalAccount` doit correspondre au compte contenant le VPC et le point de terminaison d'un VPC. La liste suivante indique comment partager le point de terminaison d'un VPC avec d'autres ID Compte AWS :

Condition d'organisation pour restreindre l'accès à votre point de terminaison

- Pour spécifier plusieurs comptes afin d'accéder au point de terminaison d'un VPC, remplacez `"aws:PrincipalAccount": "111122223333"` par ce qui suit :

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
```

```
]
```

- Pour autoriser tous les membres d'une organisation à accéder au point de terminaison d'un VPC, remplacez "aws:PrincipalAccount": "**11112223333**" par ce qui suit :

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Pour restreindre l'accès à une ressource à un ID d'organisation, ajoutez votre ResourceOrgID à la stratégie.

Pour plus d'informations, consultez la section [ResourceOrgID](#).

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Sous Paramètres supplémentaires, choisissez Activer le nom DNS.
9. Sous Sous-réseaux, choisissez les sous-réseaux dans lesquels réside votre cluster.
10. Sous Groupes de sécurité, choisissez un groupe de sécurité dont le port entrant 443 est activé depuis votre VPC (ou votre cluster EKS). Si vous ne possédez pas encore de groupe de sécurité dont le port entrant 443 est activé, [créez un groupe de sécurité](#).

En cas de problème lors de la restriction des autorisations entrantes sur votre VPC (ou instance), vous pouvez accéder au port 443 entrant depuis n'importe quelle adresse IP. (0.0.0.0/0) Il GuardDuty recommande toutefois d'utiliser des adresses IP correspondant au bloc CIDR de votre VPC. Pour plus d'informations, consultez la section [Blocs d'adresse CIDR VPC dans le guide](#) de l'utilisateur Amazon VPC.

API/CLI

Pour créer un point de terminaison VPC

- Invoquer [CreateVpcEndpoint](#).
- Utilisez les valeurs suivantes pour les paramètres :
 - Pour Nom du service, entrez **com.amazonaws.us-east-1.guardduty-data**.

Assurez-vous de le remplacer **us-east-1** par la bonne région. Il doit s'agir de la même région que le cluster EKS qui appartient à votre Compte AWS identifiant.

- Pour [DNSOptions](#), activez l'option DNS privé en la définissant sur true.
- Pour AWS Command Line Interface, voir [create-vpc-endpoint](#).

Après avoir suivi les étapes, consultez [Validation de la configuration des points de terminaison VPC](#) pour vous assurer que le point de terminaison VPC a été correctement configuré.

Installation manuelle GuardDuty de l'agent de sécurité sur les ressources Amazon EKS

Cette section décrit comment déployer l'agent de GuardDuty sécurité pour la première fois pour des clusters EKS spécifiques. Avant de passer à cette section, assurez-vous d'avoir déjà configuré les prérequis et activé la surveillance du temps d'exécution pour vos comptes. L'agent GuardDuty de sécurité (module complémentaire EKS) ne fonctionnera pas si vous n'activez pas la surveillance du temps d'exécution.

Choisissez votre méthode d'accès préférée pour déployer l'agent GuardDuty de sécurité pour la première fois.

Console

1. Ouvrez la console Amazon EKS à l'adresse <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choisissez le nom de votre cluster.
3. Cliquez sur l'onglet Add-ons.
4. Choisissez Obtenez plus de modules complémentaires.
5. Sur la page Sélectionner les modules complémentaires, choisissez Amazon GuardDuty EKS Runtime Monitoring.
6. GuardDuty recommande de choisir la version la plus récente et la plus récente de l'agent par défaut.
7. Sur la page Configurer les paramètres du module complémentaire sélectionné, utilisez les paramètres par défaut. Si le statut de votre module complémentaire EKS est Nécessite une activation, choisissez Activer GuardDuty. Cette action ouvre la GuardDuty console permettant de configurer la surveillance du temps d'exécution pour vos comptes.
8. Après avoir configuré la surveillance du temps d'exécution pour vos comptes, revenez à la console Amazon EKS. L'état de votre module complémentaire EKS doit être passé à Prêt à installer.
9. (Facultatif) Fourniture du schéma de configuration du module complémentaire EKS

Pour la version complémentaire, si vous choisissez la version v1.5.0 ou supérieure, Runtime Monitoring prend en charge la configuration de paramètres spécifiques de l' GuardDuty

agent. Pour plus d'informations sur les plages de paramètres, consultez [Configuration des paramètres du module complémentaire EKS](#).

- a. Développez les paramètres de configuration facultatifs pour afficher les paramètres configurables ainsi que leur valeur et leur format attendus.
 - b. Définissez les paramètres. Les valeurs doivent être comprises dans la plage indiquée dans [Configuration des paramètres du module complémentaire EKS](#).
 - c. Choisissez Enregistrer les modifications pour créer le module complémentaire en fonction de la configuration avancée.
 - d. Pour la méthode de résolution des conflits, l'option que vous choisissez sera utilisée pour résoudre un conflit lorsque vous mettez à jour la valeur d'un paramètre à une valeur autre que celle par défaut. Pour plus d'informations sur les options répertoriées, consultez [ResolveConflicts](#) dans le manuel Amazon EKS API Reference.
10. Choisissez Suivant.
 11. Dans la page Vérifier et créer, vérifiez tous les détails, puis choisissez Créer.
 12. Revenez aux détails du cluster et choisissez l'onglet Ressources.
 13. Vous pouvez afficher les nouveaux pods avec le préfixe aws-guardduty-agent.

API/CLI

Vous pouvez configurer l'agent de module complémentaire Amazon EKS (aws-guardduty-agent) à l'aide de l'une des options suivantes :

- Courez [CreateAddon](#) pour votre compte.

-



Note

Pour le module complémentaire `version`, si vous choisissez la version v1.5.0 ou supérieure, Runtime Monitoring prend en charge la configuration de paramètres spécifiques de l'agent GuardDuty. Pour plus d'informations, consultez [Configuration des paramètres du module complémentaire EKS](#).

Utilisez les valeurs suivantes pour les paramètres de demande :

- Pour `addonName`, saisissez `aws-guardduty-agent`.

Vous pouvez utiliser l' AWS CLI exemple suivant lorsque vous utilisez des valeurs configurables prises en charge pour les versions complémentaires v1.5.0 ou supérieures. Assurez-vous de remplacer les valeurs d'espace réservé surlignées en rouge et celles Exemple.json associées aux valeurs configurées.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.17.1-eksbuild.2 --configuration-values 'file://example.json'
```

Exemple.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

- Pour plus d'informations sur les addonVersion pris en charge, veuillez consulter [Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty](#).
- Vous pouvez également utiliser AWS CLI. Pour plus d'informations, consultez [create-addon](#).

Noms DNS privés pour le point de terminaison VPC

Par défaut, l'agent de sécurité résout et se connecte au nom DNS privé du point de terminaison VPC. Pour un point de terminaison non FIPS, votre DNS privé apparaîtra dans le format suivant :

Non-FIPS point final — guardduty-data.*us-east-1*.amazonaws.com

Le Région AWS*us-east-1*, changera en fonction de votre région.

Mise à jour manuelle de l'agent de sécurité pour les ressources Amazon EKS

Lorsque vous gérez l'agent GuardDuty de sécurité manuellement, il vous incombe de le mettre à jour pour votre compte. Pour être informé des nouvelles versions de l'agent, vous pouvez vous abonner à un flux RSS sur [GuardDuty versions publiées de l'agent de sécurité](#).

Vous pouvez mettre à jour l'agent de sécurité vers la dernière version pour bénéficier du support et des améliorations supplémentaires. Si le support standard de la version actuelle de votre agent touche à sa fin, pour continuer à utiliser Runtime Monitoring (ou EKS Runtime Monitoring), vous devez passer à la prochaine version disponible ou à la dernière version de l'agent.

Prérequis

Avant de mettre à jour la version de l'agent de sécurité, assurez-vous que la version de l'agent que vous prévoyez d'utiliser maintenant est compatible avec votre version de Kubernetes. Pour plus d'informations, consultez [Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty](#).

Console

1. Ouvrez la console Amazon EKS à l'adresse <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choisissez le nom de votre cluster.
3. Sous Informations sur le cluster, choisissez l'Add-onsonglet.
4. Sous l'Add-onsonglet, sélectionnez GuardDutyEKS Runtime Monitoring.
5. Choisissez Modifier pour mettre à jour les informations de l'agent.
6. Sur la page Configurer la surveillance du temps d'exécution GuardDuty EKS, mettez à jour les détails.
7. (Facultatif) Mise à jour des paramètres de configuration facultatifs

Si la version de votre module complémentaire EKS est 1.5.0 ou supérieure, vous pouvez également mettre à jour le schéma de configuration du module complémentaire.

- a. Développez les paramètres de configuration facultatifs pour afficher le schéma de configuration.
- b. Mettez à jour les valeurs des paramètres en fonction de la plage fournie dans [Configuration des paramètres du module complémentaire EKS](#).

- c. Choisissez Enregistrer les modifications pour démarrer la mise à jour.
- d. Pour la méthode de résolution des conflits, l'option que vous choisissez sera utilisée pour résoudre un conflit lorsque vous mettez à jour la valeur d'un paramètre à une valeur autre que celle par défaut. Pour plus d'informations sur les options répertoriées, consultez [ResolveConflicts](#) dans le manuel Amazon EKS API Reference.

API/CLI

Pour mettre à jour l'agent GuardDuty de sécurité pour vos clusters Amazon EKS, consultez la section [Mise à jour d'un module complémentaire](#).

Note

Pour le module complémentaire `version`, si vous choisissez la version 1.5.0 ou une version ultérieure, Runtime Monitoring prend en charge la configuration de paramètres spécifiques de l'agent GuardDuty. Pour plus d'informations sur les plages de paramètres, consultez [Configuration des paramètres du module complémentaire EKS](#).

Vous pouvez utiliser l'AWS CLI exemple suivant lorsque vous utilisez des valeurs configurables prises en charge pour les versions complémentaires 1.5.0 et supérieures. Assurez-vous de remplacer les valeurs d'espace réservé surlignées en rouge et celles `Example.json` associées aux valeurs configurées.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.17.1-eksbuild.2 --configuration-values 'file://example.json'
```

Example.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    }
  },
}
```

```
"limits": {  
  "cpu": "2000m",  
  "memory": "2048Mi"  
}  
}  
}
```

Si la version de votre module complémentaire Amazon EKS est 1.5.0 ou supérieure et que vous avez configuré le schéma du module complémentaire, vous pouvez vérifier si les valeurs apparaissent correctement pour votre cluster. Pour plus d'informations, consultez [Vérification des mises à jour du schéma de configuration](#).

Configuration des paramètres GuardDuty de l'agent de sécurité (module complémentaire) pour Amazon EKS

Vous pouvez configurer des paramètres spécifiques de votre agent GuardDuty de sécurité pour Amazon EKS. Ce support est disponible pour les versions 1.5.0 et supérieures de l'agent de GuardDuty sécurité. Pour plus d'informations sur les dernières versions des modules complémentaires, consultez [GuardDuty versions de l'agent de sécurité pour les ressources Amazon EKS](#).

Pourquoi dois-je mettre à jour le schéma de configuration de l'agent de sécurité

Le schéma de configuration de l'agent GuardDuty de sécurité est le même pour tous les conteneurs de vos clusters Amazon EKS. Lorsque les valeurs par défaut ne correspondent pas aux charges de travail et à la taille de l'instance associées, envisagez de configurer les paramètres du processeur `PriorityClass`, les paramètres de mémoire et `dnsPolicy` les paramètres. Quelle que soit la façon dont vous gérez l'agent GuardDuty pour vos clusters Amazon EKS, vous pouvez configurer ou mettre à jour la configuration existante de ces paramètres.

Comportement de configuration automatique des agents avec paramètres configurés

Lorsqu'il GuardDuty gère l'agent de sécurité (module complémentaire EKS) en votre nom, il met à jour le module complémentaire en fonction des besoins. GuardDuty définira la valeur des paramètres configurables sur une valeur par défaut. Cependant, vous pouvez toujours mettre à jour les paramètres à la valeur souhaitée. Si cela entraîne un conflit, l'option par défaut pour [ResolveConflicts](#) est. None

Paramètres et valeurs configurables

Pour plus d'informations sur les étapes de configuration des paramètres du module complémentaire, voir :

- [Installation manuelle GuardDuty de l'agent de sécurité sur les ressources Amazon EKS](#) ou
- [Mise à jour manuelle de l'agent de sécurité pour les ressources Amazon EKS](#)

Les tableaux suivants indiquent les plages et les valeurs que vous pouvez utiliser pour déployer le module complémentaire Amazon EKS manuellement ou pour mettre à jour les paramètres du module complémentaire existant.

Réglages du processeur

Parameters	Valeur par défaut	Gamme configurable
Requêtes	200 m	Entre 200 m et 10 000 m, les deux inclus
Restrictions	1 000 m	Entre 200 m et 10 000 m, les deux inclus
<code>disableCpuLimits</code>	<code>false</code>	<code>true</code> ou <code>false</code>

Le `disableCpuLimits` paramètre est disponible pour les versions 1.12.1-eksbuild.3 et ultérieures de l'agent de GuardDuty sécurité. Dans les versions antérieures, le module complémentaire ne prend pas en charge ce paramètre, et les API du module complémentaire Amazon EKS (`CreateAddon`, `UpdateAddon`) renvoient une erreur de validation si vous le spécifiez.

Lorsque vous définissez cette `disableCpuLimits` option `true`, le pod de l'agent de sécurité n'impose aucune limite de processeur. Les autres paramètres de ressources ne sont pas affectés.

Pour désactiver les limites du processeur, utilisez la configuration suivante :

```
{"resources":{"disableCpuLimits":true}}
```

Réglages de mémoire

Parameters	Valeur par défaut	Gamme configurable
Requêtes	256 Mi	Entre 256 mi et 20 000 mi, les deux inclus
Restrictions	1 024 milles	

Paramètres **PriorityClass**

Lorsque vous GuardDuty créez un module complémentaire Amazon EKS pour vous, le module attribué **PriorityClass** est `aws-guardduty-agent.priorityclass`. Cela signifie qu'aucune action ne sera entreprise en fonction de la priorité de l'agent pod. Vous pouvez configurer ce paramètre complémentaire en choisissant l'une des **PriorityClass** options suivantes :

Configurable PriorityClass	Valeur preemptionPolicy	preemptionPolicy description	Valeur du pod
<code>aws-guardduty-agent.priorityclass</code>	Never	Aucune action	1000000
<code>aws-guardduty-agent.priorityclass-high</code>	PreemptLowerPriority	L'attribution de cette valeur préemptera un pod exécuté avec une valeur de priorité inférieure à la valeur du pod de l'agent.	100 000 000
<code>system-cluster-critical</code> ¹	PreemptLowerPriority		2 000 000 000
<code>system-node-critical</code> ¹	PreemptLowerPriority		200 000 1000

¹ Kubernetes propose ces deux `PriorityClass` options — et `system-cluster-critical` et `system-node-critical`. Pour plus d'informations, consultez la [PriorityClass](#) documentation de Kubernetes.

Paramètres `dnsPolicy`

Choisissez l'une des options de politique DNS suivantes prises en charge par Kubernetes. Lorsqu'aucune configuration n'est spécifiée, elle `ClusterFirst` est utilisée comme valeur par défaut.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Pour plus d'informations sur ces politiques, consultez la [politique DNS de Pod](#) dans la documentation de Kubernetes.

Vérification des mises à jour du schéma de configuration

Après avoir configuré les paramètres, effectuez les étapes suivantes pour vérifier que le schéma de configuration a été mis à jour :

1. Ouvrez la console Amazon EKS à l'adresse <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le panneau de navigation, choisissez Clusters.
3. Sur la page Clusters, sélectionnez le nom du cluster dont vous souhaitez vérifier les mises à jour.
4. Sélectionnez l'onglet Ressources.
5. Dans le volet Types de ressources, sous Charges de travail, sélectionnez DaemonSets.
6. Sélectionnez `aws-guardduty-agent`.
7. Sur la page `aws-guardduty-agent`, choisissez Raw view pour afficher la réponse JSON non formatée. Vérifiez que les paramètres configurables affichent la valeur que vous avez fournie.

Après avoir vérifié, passez à la GuardDuty console. Sélectionnez le correspondant Région AWS et consultez l'état de couverture de vos clusters Amazon EKS. Pour plus d'informations, consultez [Couverture du temps d'exécution et résolution des problèmes pour les clusters Amazon EKS](#).

Validation de la configuration des points de terminaison VPC

Après avoir installé l'agent de sécurité manuellement ou par le biais d'une configuration GuardDuty automatique, vous pouvez utiliser ce document pour valider la configuration du point de terminaison VPC. Vous pouvez également suivre ces étapes après avoir résolu tout [problème de couverture d'exécution](#) pour un type de ressource. Vous pouvez vous assurer que les étapes ont fonctionné comme prévu et que le statut de couverture pourrait apparaître comme sain.

Suivez les étapes suivantes pour vérifier que la configuration du point de terminaison VPC pour votre type de ressource est correctement configurée dans le compte du propriétaire du VPC :

1. Connectez-vous à la console Amazon VPC Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/vpc/>
2. Dans le volet de navigation, sous Virtual private cloud, sélectionnez Your VPC.
3. Sur la page Vos VPC, choisissez le CIDR IPv4 associé à votre ID VPC.
4. Dans le panneau de navigation, sous Cloud privé virtuel, choisissez Points de terminaison.
5. Dans le tableau Endpoints, sélectionnez la ligne dont le nom du service est similaire à com.amazonaws. **us-east-1**.guardduty-data. La région (us-east-1) peut être différente pour votre terminal.
6. Un panneau contenant les détails du point de terminaison apparaîtra. Sous l'onglet Groupes de sécurité, sélectionnez le lien ID de groupe associé pour plus de détails.
7. Dans le tableau des groupes de sécurité, sélectionnez la ligne avec l'ID du groupe de sécurité associé pour afficher les détails.
8. Dans l'onglet Règles entrantes, assurez-vous qu'il existe une politique d'entrée avec la plage de ports 443 et la source comme valeur copiée depuis le CIDR IPv4. Les règles de trafic entrant contrôlent le trafic entrant autorisé à atteindre l'instance. L'image suivante montre les règles entrantes pour un groupe de sécurité associé au VPC utilisé par GuardDuty l'agent de sécurité.

Si vous ne possédez pas encore de groupe de sécurité dont le port entrant 443 est activé, [créez un groupe de sécurité](#) dans le guide de l'utilisateur Amazon EC2.

En cas de problème lors de la restriction des autorisations entrantes sur votre VPC (ou cluster), autorisez le trafic entrant sur le port 443 à partir de n'importe quelle adresse IP (0.0.0.0/0).

La liste suivante contient des éléments utiles à connaître après l'installation ou la mise à jour de l'agent de sécurité.

Évaluez la couverture d'exécution

Après l'installation ou la mise à jour de votre agent de sécurité, l'étape suivante consiste à évaluer la couverture d'exécution de vos ressources. Si l'état de couverture du temps d'exécution est incorrect, vous devez résoudre le problème. Pour plus d'informations, consultez [Problèmes de couverture du temps d'exécution et résolution des problèmes](#).

Si l'état de la couverture du temps d'exécution indique que Runtime Monitoring est en mesure de collecter et de recevoir des événements d'exécution. Pour obtenir la liste de ces événements, consultez [Types d'événement d'exécution collectés](#).

Nom DNS privé pour le point de terminaison

Une fois que vous avez installé l'agent de GuardDuty sécurité pour vos ressources, par défaut, il résout le problème et se connecte au nom DNS privé du point de terminaison VPC. Pour un point de terminaison non FIPS, le DNS privé apparaîtra au format suivant :

```
guardduty-data.us-east-1.amazonaws.com
```

Le Région AWS *us-east-1*, changera en fonction de votre région.

Un hôte peut être installé avec deux agents de sécurité

Lorsque vous utilisez l'agent GuardDuty de sécurité pour une instance Amazon EC2, vous pouvez installer et utiliser l'agent sur l'hôte sous-jacent au sein d'un cluster Amazon EKS. Si vous avez déjà déployé un agent de sécurité sur ce cluster EKS, deux agents de sécurité peuvent être exécutés simultanément sur le même hôte. Pour plus d'informations sur le GuardDuty fonctionnement de ce scénario, consultez [Agents de sécurité sur le même hôte](#).

Examen des statistiques de couverture du temps d'exécution et résolution des problèmes

Une fois que vous avez activé la surveillance du temps d'exécution et que l'agent de GuardDuty sécurité est déployé sur votre ressource, il GuardDuty fournit des statistiques de couverture pour le type de ressource correspondant et un état de couverture individuel pour les ressources appartenant à votre compte. L'état de couverture est déterminé en vérifiant que vous avez activé la surveillance du temps d'exécution, que votre point de terminaison Amazon VPC a été créé et que l'agent de GuardDuty sécurité pour la ressource correspondante a été déployé. Un état de couverture sain indique que lorsqu'un événement d'exécution est lié à votre ressource, GuardDuty vous êtes en

mesure de recevoir ledit événement d'exécution via le point de terminaison Amazon VPC et de surveiller le comportement. En cas de problème lors de la configuration de la surveillance du temps d'exécution, de la création d'un point de terminaison Amazon VPC ou du déploiement de l'agent de GuardDuty sécurité, l'état de couverture apparaît comme étant insalubre. Lorsque l'état de couverture est défaillant, il ne GuardDuty sera pas en mesure de recevoir ou de surveiller le comportement d'exécution de la ressource correspondante, ni de générer des résultats de surveillance du temps d'exécution.

Les rubriques suivantes vous aideront à consulter les statistiques de couverture, à configurer EventBridge les notifications et à résoudre les problèmes de couverture pour un type de ressource spécifique.

Table des matières

- [Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2](#)
- [Couverture du temps d'exécution et résolution des problèmes pour ECS-EC2 Bottlerocket](#)
- [Couverture du temps d'exécution et résolution des problèmes pour les clusters Amazon ECS](#)
- [Couverture du temps d'exécution et résolution des problèmes pour les clusters Amazon EKS](#)

Couverture du temps d'exécution et résolution des problèmes pour l'instance Amazon EC2

Pour une ressource Amazon EC2, la couverture du temps d'exécution est évaluée au niveau de l'instance. Vos instances Amazon EC2 peuvent exécuter plusieurs types d'applications et de charges de travail, entre autres, dans votre environnement. AWS Cette fonctionnalité prend également en charge les instances Amazon EC2 gérées par Amazon ECS et si vous avez des clusters Amazon ECS exécutés sur une instance Amazon EC2, les problèmes de couverture au niveau de l'instance apparaîtront dans le cadre de la couverture d'exécution Amazon EC2.

Rubriques

- [Consultation des statistiques de couverture](#)
- [Modification de l'état de couverture avec EventBridge notifications](#)
- [Résolution des problèmes de couverture des environnements d'exécution Amazon EC2](#)

Consultation des statistiques de couverture

Les statistiques de couverture pour les instances Amazon EC2 associées à vos propres comptes ou à vos comptes membres sont le pourcentage d'instances EC2 saines par rapport à toutes les instances EC2 de la sélection. Région AWS L'équation suivante représente cela comme suit :

$(\text{instances}/\text{All Instances saines}) * 100$

Si vous avez également déployé l'agent de GuardDuty sécurité pour vos clusters Amazon ECS, tout problème de couverture au niveau de l'instance associé aux clusters Amazon ECS exécutés sur une instance Amazon EC2 apparaîtra comme un problème de couverture du temps d'exécution de l'instance Amazon EC2.

Choisissez l'une des méthodes d'accès pour consulter les statistiques de couverture de vos comptes.

Console

- Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
- Dans le volet de navigation, choisissez Runtime Monitoring.
- Choisissez l'onglet Runtime coverage.
- Dans l'onglet Couverture du temps d'exécution des instances EC2, vous pouvez consulter les statistiques de couverture agrégées en fonction de l'état de couverture de chaque instance Amazon EC2 disponible dans le tableau de liste des instances.
 - Vous pouvez filtrer le tableau de la liste des instances selon les colonnes suivantes :
 - ID de compte
 - Type de gestion des agents
 - Version de l'agent
 - État de couverture
 - ID de l'instance
 - ARN du cluster
- Si l'état de couverture de l'une de vos instances EC2 est considéré comme défaillant, la colonne Problème inclut des informations supplémentaires sur la raison de ce statut d'insalubrité.

API/CLI

- Exécutez l'[ListCoverage](#) API avec votre propre identifiant de détecteur valide, votre région actuelle et votre point de terminaison de service. Vous pouvez filtrer et trier la liste des instances à l'aide de cette API.
- Vous pouvez modifier l'exemple de `filter-criteria` à l'aide de l'une des options suivantes pour `CriterionKey` :
 - `ACCOUNT_ID`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `AGENT_VERSION`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
 - `CLUSTER_ARN`
- Lorsqu'il est `filter-criteria` inclus `RESOURCE_TYPE` en tant qu'EC2, Runtime Monitoring ne prend pas en charge l'utilisation de `ISSUE` en tant que `AttributeName`. Si vous l'utilisez, la réponse de l'API en résultera `InvalidInputException`.

Vous pouvez modifier l'exemple de `AttributeName` dans `sort-criteria` à l'aide des options suivantes :

- `ACCOUNT_ID`
- `COVERAGE_STATUS`
- `INSTANCE_ID`
- `UPDATED_AT`
- Vous pouvez modifier le *`max-results`* (jusqu'à 50).
- `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}] }' --max-results 5
```

- Exécutez l'[GetCoverageStatistics](#) API pour récupérer les statistiques agrégées de couverture sur la base de `statisticsType`.
- Vous pouvez modifier l'exemple de `statisticsType` sur l'une des options suivantes :
 - `COUNT_BY_COVERAGE_STATUS` : représente les statistiques de couverture pour les clusters EKS agrégées par état de couverture.
 - `COUNT_BY_RESOURCE_TYPE`— Statistiques de couverture agrégées en fonction du type de AWS ressource figurant dans la liste.
- Vous pouvez modifier l'exemple de `filter-criteria` dans la commande. Vous pouvez utiliser les options suivantes pour `CriterionKey` :
 - `ACCOUNT_ID`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `AGENT_VERSION`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
 - `CLUSTER_ARN`
- `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si l'état de couverture de votre instance EC2 n'est pas satisfaisant, consultez [Résolution des problèmes de couverture des environnements d'exécution Amazon EC2](#).

Modification de l'état de couverture avec EventBridge notifications

L'état de couverture de votre instance Amazon EC2 peut apparaître comme étant défectueux. Pour savoir quand l'état de couverture change, nous vous recommandons de le surveiller régulièrement et de résoudre les problèmes s'il devient insalubre. Vous pouvez également créer une EventBridge règle Amazon pour recevoir une notification lorsque le statut de couverture passe de Malsain à Sain ou autre. Par défaut, il le GuardDuty publie dans le [EventBridge bus](#) pour votre compte.

Exemple de schéma de notification

Dans une EventBridge règle, vous pouvez utiliser les exemples d'événements et de modèles d'événements prédéfinis pour recevoir une notification de l'état de couverture. Pour plus d'informations sur la création d'une EventBridge règle, consultez la section [Créer une règle](#) dans le guide de EventBridge l'utilisateur Amazon.

En outre, vous pouvez créer un modèle d'événement personnalisé à l'aide de l'exemple de schéma de notification suivant. Assurez-vous de remplacer les valeurs de votre compte. Pour être averti lorsque le statut de couverture de votre instance Amazon EC2 passe de Healthy à Unhealthy, le detail-type doit être. *GuardDuty Runtime Protection Unhealthy* Pour être averti lorsque le statut de couverture passe de Unhealthy à Healthy, remplacez la valeur de detail-type par *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Compte AWS ID",
  "time": "event timestamp (string)",
  "region": "Région AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EC2",
      "ec2InstanceDetails": {
        "instanceId": "",
        "instanceType": "",
        "clusterArn": "",
        "agentDetails": {
          "version": ""
        },
        "managementType": ""
      }
    },
    "issue": "string",
```

```

    "lastUpdatedAt": "timestamp"
  }
}

```

Résolution des problèmes de couverture des environnements d'exécution Amazon EC2

Si l'état de couverture de votre instance Amazon EC2 n'est pas satisfaisant, vous pouvez en connaître la raison dans la colonne Problème.

Si votre instance EC2 est associée à un cluster EKS et que l'agent de sécurité pour EKS a été installé manuellement ou via une configuration automatique de l'agent, pour résoudre le problème de couverture, consultez. [Couverture du temps d'exécution et résolution des problèmes pour les clusters Amazon EKS](#)

Le tableau suivant répertorie les types de problèmes et les étapes de dépannage correspondantes.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Aucun signalement par un agent	En attente d'une notification par SMS	La réception de la notification SSM peut prendre quelques minutes. Assurez-vous que l'instance Amazon EC2 est gérée par SSM. Pour plus d'informations, consultez les étapes décrites dans la section Méthode 1 - À l'aide de AWS Systems Manager dans Installation manuelle de l'agent de sécurité .
	(Vide exprès)	Si vous gérez l'agent GuardDuty de sécurité manuellement, assurez-vous d'avoir suivi les étapes ci-dessous Gestion manuelle

Type de problème	Message d'émission	Étapes de résolution des problèmes
		<p>de l'agent de sécurité pour la ressource Amazon EC2.</p> <p>Si vous avez activé la configuration automatique des agents :</p> <ul style="list-style-type: none">• Votre instance EC2 est gérée par SSM.• Consultez régulièrement le statut de votre agent de sécurité. Pour plus d'informations, consultez Validation de l'état d'installation GuardDuty de l'agent de sécurité. <p>Vérifiez que le point de terminaison VPC de votre instance Amazon EC2 est correctement configuré. Pour plus d'informations, consultez Validation de la configuration des points de terminaison VPC.</p>

Type de problème	Message d'émission	Étapes de résolution des problèmes
		<p>Si votre organisation dispose d'une politique de contrôle des services (SCP), vérifiez que la limite des autorisations ne restreint pas les guardduty :SendSecurityTelemetry autorisations. Pour plus d'informations, consultez Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes.</p>

Type de problème	Message d'émission	Étapes de résolution des problèmes
	Agent déconnecté	<ul style="list-style-type: none"> Consultez le statut de votre agent de sécurité. Pour plus d'informations, consultez Validation de l'état d'installation GuardDuty de l'agent de sécurité. Consultez les journaux des agents de sécurité pour identifier la cause première potentielle. Les journaux fournissent des erreurs détaillées que vous pouvez utiliser pour résoudre le problème vous-même. Les fichiers journaux sont disponibles sous <code>/var/log/amzn-guardduty-agent/</code>. <p>Faissudo <code>journalctl -u amazon-guardduty-agent</code>.</p>
Agent non provisionné	Les instances comportant des balises d'exclusion sont exclues de la surveillance du temps d'exécution.	<p>GuardDuty ne reçoit pas d'événements d'exécution provenant d'instances Amazon EC2 lancées avec la balise d'exclusion <code>:GuardDutyManaged</code> <code>. false</code></p> <p>Pour recevoir les événements d'exécution de cette instance Amazon EC2, supprimez la balise d'exclusion.</p>

Type de problème	Message d'émission	Étapes de résolution des problèmes
	La version du noyau est inférieure à la version prise en charge.	Pour plus d'informations sur les versions de noyau prises en charge par les distributions du système d'exploitation, consultez Valider les exigences architecturales la section consacrée aux instances Amazon EC2.
	La version du noyau est supérieure à la version prise en charge.	Pour plus d'informations sur les versions de noyau prises en charge par les distributions du système d'exploitation, consultez Valider les exigences architecturales la section consacrée aux instances Amazon EC2.

Type de problème	Message d'émission	Étapes de résolution des problèmes
	Impossible de récupérer le document d'identité de l'instance.	<p>Procédez comme suit :</p> <ol style="list-style-type: none">1. Vérifiez que votre ressource est une instance Amazon EC2 et non une instance hybride non EC2.2. Vérifiez que le service de métadonnées d'instance (IMDS) est activé. Pour ce faire, consultez la section Configurer les options du service de métadonnées d'instance dans le guide de l'utilisateur Amazon EC2.3. Vérifiez que le document d'identité de l'instance existe. Pour ce faire, consultez la section Récupérer le document d'identité de l'instance dans le guide de l'utilisateur Amazon EC2.4. Si le document d'identité de l'instance n'existe toujours pas, redémarrez l'instance. Le document d'identité d'instance est généré lorsque l'instance est arrêtée et démarrée, redémarrée ou lancée.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de la création de l'association SSM	GuardDuty L'association SSM existe déjà dans votre compte	<ol style="list-style-type: none">1. Supprimez manuellement l'association existante . Pour plus d'informations, consultez la section Suppression d'associations dans le guide de AWS Systems Manager l'utilisateur.2. Après avoir supprimé l'association, désactivez puis réactivez la configuration GuardDuty automatique de l'agent pour Amazon EC2.
	Votre compte comporte trop d'associations SSM	<p>Choisissez l'une des deux options suivantes :</p> <ul style="list-style-type: none">• Supprimez toutes les associations SSM non utilisées. Pour plus d'informations, consultez la section Suppression d'associations dans le guide de AWS Systems Manager l'utilisateur.• Vérifiez si votre compte est éligible à une augmentation de quota. Pour plus d'informations, consultez la section Quotas du service Systems Manager dans le Références générales AWS.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de la mise à jour de l'association SSM	GuardDuty L'association SSM n'existe pas dans votre compte	GuardDuty L'association SSM n'est pas présente dans votre compte. Désactivez puis réactivez la surveillance du temps d'exécution.
Echec de la suppression de l'association SSM	GuardDuty L'association SSM n'existe pas dans votre compte	L'association SSM n'est pas présente dans votre compte. Si l'association SSM a été supprimée intentionnellement, aucune action n'est nécessaire.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de l'exécution de l'association d'instances SSM	Les exigences architecturales ou autres prérequis ne sont pas respectés.	<p>Pour plus d'informations sur les distributions de systèmes d'exploitation vérifiées, consultez Conditions préalables à la prise en charge des instances Amazon EC2.</p> <p>Si le problème persiste, les étapes suivantes vous aideront à l'identifier et éventuellement à le résoudre :</p> <ol style="list-style-type: none">1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.2. Dans le volet de navigation, sous Gestion des nœuds, sélectionnez State Manager.3. Filtrez par propriété Nom du document et entrez AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.4. Sélectionnez l'ID d'association correspondant et consultez son historique d'exécution.5. À l'aide de l'historique des exécutions, visualisez les

Type de problème	Message d'émission	Étapes de résolution des problèmes
		échecs, identifiez la cause première potentielle et essayez de la résoudre.
Échec de la création du point de terminaison VPC	La création de points de terminaison VPC n'est pas prise en charge pour les VPC partagés <i>vpcId</i>	La surveillance du temps d'exécution prend en charge l'utilisation d'un VPC partagé au sein d'une organisation. Pour plus d'informations, consultez Utilisation d'un VPC partagé avec surveillance du temps d'exécution .
	Uniquement lors de l'utilisation d'un VPC partagé avec configuration d'agent automatisée L'ID <i>111122223333</i> de compte propriétaire du VPC partagé <i>vpcId</i> n'est activé ni la surveillance du temps d'exécution, ni la configuration automatique des agents, ni les deux	Le compte propriétaire du VPC partagé doit activer la surveillance du temps d'exécution et la configuration automatique des agents pour au moins un type de ressource (Amazon EKS ou Amazon ECS (AWS Fargate)). Pour plus d'informations, consultez Prérequis spécifiques à la surveillance du temps d' GuardDuty exécution .

Type de problème	Message d'émission	Étapes de résolution des problèmes
	<p>L'activation du DNS privé nécessite à la fois que <code>enableDnsSupport</code> et les attributs <code>enableDnsHostnames</code> du VPC soient définis sur <code>true</code> pour <i>vpcId</i> (Service : Ec2, Status Code:400, Request ID :). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i></p>	<p>Assurez-vous que les attributs de VPC suivants sont définis sur <code>true</code> : <code>enableDnsSupport</code> et <code>enableDnsHostnames</code> . Pour plus d'informations, veuillez consulter la rubrique Attributs DNS dans votre VPC.</p> <p>Si vous utilisez la console Amazon VPC https://console.aws.amazon.com/vpc/ pour créer l'Amazon VPC, sélectionnez Activer les noms d'hôte DNS et Activer la résolution DNS. Pour plus d'informations, veuillez consulter Options de configuration de VPC.</p> <p>Après avoir mis à jour les attributs du VPC, vous devez accélérer la nouvelle tentative de création du point de terminaison VPC en apportant l'une des modifications suivantes :</p> <ul style="list-style-type: none"> • Vous pouvez ajouter ou modifier le <code>GuardDutyManaged</code> tag pour votre instance Amazon EC2 (recommandé). Par exemple, vous pouvez ajouter GuardDuty

Type de problème	Message d'émission	Étapes de résolution des problèmes
		<p>Managed : <code>true</code> pour inclure l'instance de surveillance du temps d'exécution.</p> <ul style="list-style-type: none">• Vous pouvez modifier l'état de l'instance Amazon EC2 (arrêt ou redémarrage).

Type de problème	Message d'émission	Étapes de résolution des problèmes
La suppression du point de terminaison VPC partagé a échoué	La suppression du point de terminaison VPC partagé n'est pas autorisée pour l'ID de compte 111122223333 , le VPC vpcId partagé et l'ID de compte propriétaire. 555555555555	<p>Étapes potentielles :</p> <ul style="list-style-type: none"> La désactivation de l'état de surveillance du temps d'exécution du compte de participant VPC partagé n'a aucun impact sur la politique de point de terminaison du VPC partagé ni sur le groupe de sécurité existant dans le compte propriétaire. <p>Pour supprimer le point de terminaison et le groupe de sécurité VPC partagés, vous devez désactiver la surveillance du temps d'exécution ou l'état de configuration automatique de l'agent dans le compte propriétaire du VPC partagé.</p> <ul style="list-style-type: none"> Le compte de participant VPC partagé ne peut pas supprimer le point de terminaison et le groupe de sécurité VPC partagés hébergés dans le compte propriétaire du VPC partagé.

Type de problème	Message d'émission	Étapes de résolution des problèmes
L'agent ne fait pas de rapport	(Vide exprès)	<p>Le type de problème a atteint la fin du support. Si le problème persiste et que ce n'est pas déjà fait, activez l'agent GuardDuty automatique pour Amazon EC2.</p> <p>Si le problème persiste, pensez à désactiver la surveillance du temps d'exécution pendant quelques minutes, puis réactivez-la.</p>

Couverture du temps d'exécution et résolution des problèmes pour ECS-EC2 Bottlerocket

Pour les instances Bottlerocket Amazon EC2 dans les clusters Amazon ECS GuardDuty, évalue la couverture d'exécution au niveau de l'instance. L'agent GuardDuty de sécurité s'exécute en tant que conteneur hôte sur Bottlerocket, plutôt qu'en tant que paquet RPM ou Debian installé.

Les instances Bottlerocket Amazon EC2 apparaissent sous l'onglet Couverture du temps d'exécution des instances EC2. Pour consulter les statistiques de couverture de vos instances Bottlerocket, ouvrez la GuardDuty console, choisissez Runtime Monitoring dans le volet de navigation, puis choisissez l'onglet Runtime coverage. Dans le cadre de la couverture du temps d'exécution des instances EC2, vous pouvez consulter l'état de couverture de chaque instance et filtrer par ID de compte, version de l'agent ou statut de couverture. Pour plus d'informations, consultez [Consultation des statistiques de couverture](#).

Résolution des problèmes de couverture d'exécution de Bottlerocket ECS-EC2

Si l'état de couverture de votre instance Bottlerocket Amazon EC2 est défectueux, vous pouvez en voir la raison dans la colonne Problème.

Le tableau suivant répertorie les types de problèmes et les étapes de dépannage correspondantes.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Aucun signalement par un agent	En attente d'une notification par SMS	<p>La réception de la notification SSM peut prendre quelques minutes.</p> <p>Assurez-vous que votre instance Bottlerocket est gérée par SSM. L'agent SSM s'exécute dans le conteneur de contrôle Bottlerocket par défaut. Vérifiez que le profil d'instance inclut les politiques AmazonEC2ContainerRegistryReadOnly gérées AmazonSSM ManagedInstanceCore et.</p>
Aucun signalement par un agent	Non applicable	<p>Vérifiez que le conteneur hôte de l'agent est activé et en cours d'exécution :</p> <ol style="list-style-type: none"> 1. Connectez-vous à votre instance à l'aide du gestionnaire de session SSM. 2. Entrez le conteneur d'administration : <code>enter-admin-container</code> . 3. Vérifiez les paramètres : <code>apiclient get settings.host-containers.amazon-guardduty-agent</code> . Confirmez que

Type de problème	Message d'émission	Étapes de résolution des problèmes
		<p><code>c'enabledest true</code> et que <code>c'superpowered</code> est le <code>castrue</code>.</p> <p>4. Vérifiez si le processus de l'agent est en cours d'exécution : <code>sheltie ps aux grep guardduty</code>.</p> <p>5. Consultez les journaux des agents à l'aide de l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • <code>sheltie journalctl -u host-container@amazon-guardduty-agent</code> • À partir d'une session Sheltie (<code>sudo sheltie</code>) : <code>ls /var/log/amzn-guardduty-agent/</code>.
Aucun signalement par un agent	Non applicable	<p>Vérifiez que l'instance dispose d'une connectivité réseau avec le point de terminaison Amazon ECR et le point de terminaison GuardDuty VPC. Si votre instance s'exécute dans un sous-réseau privé, assurez-vous d'avoir configuré les points de terminaison VPC pour Amazon ECR et GuardDuty.</p>

Type de problème	Message d'émission	Étapes de résolution des problèmes
Aucun signalement par un agent	Non applicable	Si votre organisation dispose d'une politique de contrôle des services (SCP), vérifiez que la limite des autorisations autorise l'guardduty :SendSecurityTelemetry autorisation.
Échec de la création de l'association SSM	GuardDuty L'association SSM existe déjà dans votre compte.	<ol style="list-style-type: none">1. Supprimez manuellement l'association existante . Pour plus d'informations, consultez la section Suppression d'associations dans le guide de AWS Systems Manager l'utilisateur.2. Après avoir supprimé l'association, désactivez puis réactivez la configuration GuardDuty automatique de l'agent pour Amazon EC2.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de la création de l'association SSM	Votre compte comporte un trop grand nombre d'associations SSM.	<p>Choisissez l'une des deux options suivantes :</p> <ul style="list-style-type: none"> Supprimez toutes les associations SSM non utilisées. Pour plus d'informations, consultez la section Suppression d'associations dans le guide de AWS Systems Manager l'utilisateur. Vérifiez si votre compte est éligible à une augmentation de quota. Pour plus d'informations, consultez la section Quotas du service Systems Manager dans le Références générales AWS.
La mise à jour de l'association SSM a échoué	GuardDuty L'association SSM n'existe pas dans votre compte.	GuardDuty L'association SSM n'est pas présente dans votre compte. Désactivez puis réactivez la surveillance du temps d'exécution.
Echec de la suppression de l'association SSM	GuardDuty L'association SSM n'existe pas dans votre compte.	L'association SSM n'est pas présente dans votre compte. Si l'association SSM a été supprimée intentionnellement, aucune action n'est nécessaire.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de l'exécution de l'association d'instances SSM	Les exigences architecturales ou autres prérequis ne sont pas respectés.	<p>Pour plus d'informations sur les exigences vérifiées, consultez Conditions préalables au support de ECS-EC2 Bottlerocket.</p> <p>Si le problème persiste, consultez l'historique d'exécution de SSM State Manager :</p> <ol style="list-style-type: none">1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.2. Dans le volet de navigation, sous Gestion des nœuds, sélectionnez State Manager.3. Filtrez par propriété Nom du document et entrez AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.4. Sélectionnez l'ID d'association correspondant et consultez son historique d'exécution.5. À l'aide de l'historique des exécutions, visualisez les échecs, identifiez la cause

Type de problème	Message d'émission	Étapes de résolution des problèmes
		première potentielle et essayez de la résoudre.
Agent déconnecté	Non applicable	<ul style="list-style-type: none">• Vérifiez les journaux des agents depuis le conteneur d'administration :<div><pre>enter-admin-contai ner sheltie journalctl - u host-containers@am azon-guardduty-age nt</pre></div>• Vérifiez que l'image du conteneur de l'agent a été correctement extraite en vérifiant que le source champ dans les paramètres du conteneur hôte pointe vers un URI Amazon ECR valide.• Assurez-vous que le profil d'instance dispose des autorisations d'extraction Amazon ECR. Pour plus d'informations, consultez Gérer les instances EC2 par SSM et configurer les autorisations des instances.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Agent non provisionné	Les instances comportant des balises d'exclusion sont exclues de la surveillance du temps d'exécution.	<p>GuardDuty ne reçoit pas d'événements d'exécution provenant d'instances Amazon EC2 lancées avec la balise d'exclusion :GuardDuty Managed . false</p> <p>Pour recevoir les événements d'exécution de cette instance, supprimez la balise d'exclusion.</p>
Agent non provisionné	La version du noyau est inférieure à la version prise en charge.	Passez à la dernière version de Bottlerocket ou à une ECS-3 AMI ECS-2 optimisée v1.62.1 ou à une version ultérieure pour une configuration automatique des agents.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de l'extraction de l'image ECR	L'image du conteneur de l'agent n'a pas pu être extraite d'Amazon ECR.	<ul style="list-style-type: none">• Vérifiez que le profil d'instance inclut la politique AmazonEC2ContainerRegistryReadOnly gérée ou les autorisations individuelles Amazon ECR requises.• Vérifiez la connectivité réseau au point de terminaison Amazon ECR de votre région.• Si vous utilisez un sous-réseau privé, assurez-vous que les points de terminaison VPC sont configurés. Pour plus d'informations, consultez Exigences en matière de connectivité réseau.

Couverture du temps d'exécution et résolution des problèmes pour les clusters Amazon ECS

La couverture d'exécution des clusters Amazon ECS inclut les tâches exécutées sur les instances de conteneur Amazon ECS AWS Fargate et sur celles-ci ¹.

Pour un cluster Amazon ECS qui s'exécute sur Fargate, la couverture d'exécution est évaluée au niveau de la tâche. La couverture du temps d'exécution des clusters ECS inclut les tâches Fargate qui ont commencé à s'exécuter une fois que vous avez activé la surveillance du temps d'exécution et la configuration automatisée des agents pour Fargate (ECS uniquement). Par défaut, une tâche Fargate est immuable. GuardDuty ne sera pas en mesure d'installer l'agent de sécurité pour surveiller les conteneurs sur les tâches déjà en cours d'exécution. Pour inclure une telle tâche Fargate, vous

devez arrêter puis recommencer la tâche. Assurez-vous de vérifier si le service associé est pris en charge.

Pour plus d'informations sur le conteneur Amazon ECS, consultez la section [Création de capacités](#).

Table des matières

- [Consultation des statistiques de couverture](#)
- [Modification de l'état de couverture avec EventBridge notifications](#)
- [Résolution des problèmes de couverture du ECS-Fargate temps d'exécution d'Amazon](#)

Consultation des statistiques de couverture

Les statistiques de couverture pour les ressources Amazon ECS associées à votre propre compte ou à vos comptes de membres sont le pourcentage de clusters Amazon ECS sains par rapport à tous les clusters Amazon ECS du groupe sélectionné Région AWS. Cela inclut la couverture des clusters Amazon ECS associés à la fois aux instances Fargate et Amazon EC2. L'équation suivante représente cela comme suit :

$(\text{clusters/All Clusters sains}) * 100$

Considérations

- Les statistiques de couverture du cluster ECS incluent l'état de couverture des tâches Fargate ou des instances de conteneur ECS associées à ce cluster ECS. L'état de couverture des tâches Fargate inclut les tâches en cours d'exécution ou récemment terminées.
- Dans l'onglet Couverture d'exécution des clusters ECS, le champ Instances de conteneur couvertes indique l'état de couverture des instances de conteneur Amazon EC2 associées à votre cluster Amazon ECS.

Si votre cluster Amazon ECS exécute uniquement le type de lancement Fargate, ce champ affiche un tiret (-) pour indiquer que le nombre n'est pas applicable. Un Fargate-only cluster n'a aucune instance de conteneur Amazon EC2 à couvrir.

- Si votre cluster Amazon ECS est associé à une instance Amazon EC2 dépourvue d'agent de sécurité, le cluster Amazon ECS aura également un statut de couverture défaillant.

Pour identifier et résoudre le problème de couverture de l'instance Amazon EC2 associée, [Résolution des problèmes de couverture des environnements d'exécution Amazon EC2](#) consultez la section consacrée aux instances Amazon EC2.

Choisissez l'une des méthodes d'accès pour consulter les statistiques de couverture de vos comptes.

Console

- Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
- Dans le volet de navigation, choisissez Runtime Monitoring.
- Choisissez l'onglet Runtime coverage.
- Dans l'onglet Couverture d'exécution des clusters ECS, vous pouvez consulter les statistiques de couverture agrégées en fonction de l'état de couverture de chaque cluster Amazon ECS disponible dans le tableau de liste des clusters.
 - Vous pouvez filtrer le tableau de liste des clusters selon les colonnes suivantes :
 - ID de compte
 - Nom du cluster
 - Type de gestion des agents
 - État de couverture
- Si l'état de couverture de l'un de vos clusters Amazon ECS est considéré comme insalubre, la colonne Problème inclut des informations supplémentaires sur la raison de ce statut insalubre.

Si vos clusters Amazon ECS sont associés à une instance Amazon EC2, accédez à l'onglet Couverture du temps d'exécution de l'instance EC2 et filtrez par le champ Nom du cluster pour afficher le problème associé.

API/CLI

- Exécutez l'[ListCoverage](#) API avec votre propre identifiant de détecteur valide, votre région actuelle et votre point de terminaison de service. Vous pouvez filtrer et trier la liste des instances à l'aide de cette API.
- Vous pouvez modifier l'exemple de `filter-criteria` à l'aide de l'une des options suivantes pour `CriterionKey` :
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`

- Vous pouvez modifier l'exemple de `AttributeName` dans `sort-criteria` à l'aide des options suivantes :
 - `ACCOUNT_ID`
 - `COVERAGE_STATUS`
 - `ISSUE`
 - `ECS_CLUSTER_NAME`
 - `UPDATED_AT`

Le champ est mis à jour uniquement lorsqu'une nouvelle tâche est créée dans le cluster Amazon ECS associé ou en cas de modification de l'état de couverture correspondant.

- Vous pouvez modifier le *max-results* (jusqu'à 50).
- `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"} } ]}' --max-results 5
```

- Exécutez l'[GetCoverageStatistics](#) API pour récupérer les statistiques agrégées de couverture sur la base `statisticsType`.
- Vous pouvez modifier l'exemple de `statisticsType` sur l'une des options suivantes :
 - `COUNT_BY_COVERAGE_STATUS`— Représente les statistiques de couverture pour les clusters ECS agrégées par état de couverture.
 - `COUNT_BY_RESOURCE_TYPE`— Statistiques de couverture agrégées en fonction du type de AWS ressource figurant dans la liste.
- Vous pouvez modifier l'exemple de `filter-criteria` dans la commande. Vous pouvez utiliser les options suivantes pour `CriterionKey` :
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`

- `INSTANCE_ID`
- `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Pour plus d'informations sur les problèmes de couverture, consultez [Résolution des problèmes de couverture du ECS-Fargate temps d'exécution d'Amazon](#).

Modification de l'état de couverture avec EventBridge notifications

L'état de couverture de votre cluster Amazon ECS peut apparaître comme étant défectueux. Pour savoir quand l'état de couverture change, nous vous recommandons de le surveiller régulièrement et de résoudre les problèmes s'il devient insalubre. Vous pouvez également créer une EventBridge règle Amazon pour recevoir une notification lorsque le statut de couverture passe de Malsain à Sain ou autre. Par défaut, il le GuardDuty publie dans le [EventBridge bus](#) pour votre compte.

Exemple de schéma de notification

Dans une EventBridge règle, vous pouvez utiliser les exemples d'événements et de modèles d'événements prédéfinis pour recevoir une notification de l'état de couverture. Pour plus d'informations sur la création d'une EventBridge règle, consultez la section [Créer une règle](#) dans le guide de EventBridge l'utilisateur Amazon.

En outre, vous pouvez créer un modèle d'événement personnalisé à l'aide de l'exemple de schéma de notification suivant. Assurez-vous de remplacer les valeurs de votre compte. Pour être averti lorsque le statut de couverture de votre cluster Amazon ECS passe de Healthy à Unhealthy, le `detail-type` doit être *GuardDuty Runtime Protection Unhealthy*. Pour être averti lorsque le statut de couverture passe de Unhealthy à Healthy, remplacez la valeur de `detail-type` par *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
```

```

"detail-type": "GuardDuty Runtime Protection Unhealthy",
"source": "aws.guardduty",
"account": "Compte AWS ID",
"time": "event timestamp (string)",
"region": "Région AWS",
"resources": [
  ],
"detail": {
  "schemaVersion": "1.0",
  "resourceAccountId": "string",
  "currentStatus": "string",
  "previousStatus": "string",
  "resourceDetails": {
    "resourceType": "ECS",
    "ecsClusterDetails": {
      "clusterName": "",
      "fargateDetails": {
        "issues": [],
        "managementType": ""
      },
      "containerInstanceDetails": {
        "coveredContainerInstances": int,
        "compatibleContainerInstances": int
      }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}

```

Résolution des problèmes de couverture du ECS-Fargate temps d'exécution d'Amazon

Si l'état de couverture de votre cluster Amazon ECS n'est pas satisfaisant, vous pouvez en connaître la raison dans la colonne Problème.

Le tableau suivant fournit les étapes de dépannage recommandées pour les problèmes liés à Fargate (Amazon ECS uniquement). Pour plus d'informations sur les problèmes de couverture des instances Amazon EC2, consultez la section relative [Résolution des problèmes de couverture des environnements d'exécution Amazon EC2](#) aux instances Amazon EC2.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
L'agent ne fait pas de rapport	L'agent ne présente pas de rapports pour les tâches dans TaskDefinition - <code>'TASK_DEFINITION'</code>	<p>Vérifiez que le point de terminaison VPC pour la tâche de votre cluster Amazon ECS est correctement configuré . Pour plus d'informations, consultez Validation de la configuration des points de terminaison VPC.</p> <p>Si votre organisation dispose d'une politique de contrôle des services (SCP), vérifiez que la limite des autorisations ne restreint pas les guardduty :SendSecurityTelemetry autorisations. Pour plus d'informations, consultez Validation de la politique de contrôle des services de votre organisation dans un environnement multi-comptes.</p>
	<code>VPC_ISSUE ; for task in TaskDefinition - 'TASK_DEFINITION'</code>	Consultez les détails du problème du VPC dans les informations supplémentaires.
L'agent est sorti	ExitCode: EXIT_CODE pour les tâches dans TaskDefinition - <code>'TASK_DEFINITION'</code>	Consultez les détails du problème dans les informations supplémentaires.
	Motif : <code>REASON</code> pour les tâches dans TaskDefinition - <code>'TASK_DEFINITION'</code>	

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	ExitCode: EXIT_CODE avec raison : « <i>EXIT_CODE</i> » pour les tâches dans TaskDefinition - ' <i>TASK_DEFINITION</i> '	

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	L'agent est sorti : Raison <code>CannotPullContainerError</code> : le manifeste de l'image d'extraction a été réessayé...	<p>Dans ce scénario, GuardDuty il est potentiellement impossible d'extraire l'image du conteneur du sidecar. Votre tâche continuera de s'exécuter mais ne GuardDuty pourra pas détecter les menaces potentielles. Effectuez les étapes de dépannage suivantes une par une pour vérifier si cela permet de résoudre le problème de couverture :</p> <ul style="list-style-type: none"> • Autorisations : assurez-vous que votre rôle d'exécution de tâches dispose des autorisations ECR requises répertoriées dans Conditions d'autorisation. • Connectivité réseau : vérifiez que vos tâches Fargate peuvent atteindre ECR via un accès Internet public ou via des points de terminaison VPC correctement configurés, comme décrit dans Exigences en matière de connectivité réseau • Configuration du groupe de sécurité : Vérifiez que votre groupe de sécurité autorise l'accès sortant à la liste des

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
		<p>préfixes gérés S3 sur le port 443, comme expliqué dans. Configuration du groupe de sécurité</p> <ul style="list-style-type: none">• Exécutez le AWS Support-TroubleshootECSTaskFailedToStart runbook dans la région de votre cluster pour identifier les problèmes spécifiques.• Consultez les journaux des tâches pour détecter les messages d'erreur. Pour plus d'informations sur la procédure à suivre, consultez la section Affichage des journaux des agents de conteneur Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide. <p>Pour les erreurs courantes et le dépannage, consultez la section relative à la résolution des problèmes liés à Amazon ECS dans le manuel du développeur Amazon Elastic Container Service.</p>

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
		<p>Ces trois composants (autorisations, connectivité réseau et configuration du groupe de sécurité) sont indépendants mais tous nécessaires pour télécharger correctement l'image du GuardDuty conteneur depuis Amazon ECR.</p> <p>Si le problème persiste, consultez Mon AWS Step Functions le flux de travail échoue de façon inattendue.</p>
Échec de la création du point de terminaison VPC	<p>L'activation du DNS privé nécessite à la fois que <code>enableDnsSupport</code> les attributs <code>enableDnsHostnames</code> VPC soient définis sur <code>true</code> for <i>vpcId</i> (Service : EC2, Status Code:400, Request ID :). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i></p>	<p>Assurez-vous que les attributs de VPC suivants sont définis sur <code>true</code> : <code>enableDnsSupport</code> et <code>enableDnsHostnames</code> . Pour plus d'informations, veuillez consulter la rubrique Attributs DNS dans votre VPC.</p> <p>Si vous utilisez la console Amazon VPC https://console.aws.amazon.com/vpc/ pour créer l'Amazon VPC, assurez-vous de sélectionner à la fois Activer les noms d'hôte DNS et Activer la résolution DNS. Pour plus d'informations, veuillez consulter Options de configuration de VPC.</p>

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
Agent non provisionné	Invocation non prise en charge par SERVICE for task (s) dans TaskDefinition - 'TASK_DEFINITION'	Cette tâche a été invoquée par une tâche SERVICE qui n'est pas prise en charge.
	Architecture de processeur « TYPE » non prise en charge pour les tâches dans TaskDefinition - 'TASK_DEFINITION'	Cette tâche est exécutée sur une architecture de processeur non prise en charge. Pour plus d'informations sur les architectures de processeur prises en charge, consultez Validation des exigences architecturales .
	TaskExecutionRole absent de TaskDefinition - 'TASK_DEFINITION'	Le rôle d'exécution des tâches ECS est absent. Pour plus d'informations sur la fourniture du rôle d'exécution des tâches et des autorisations requises, consultez Conditions préalables à l'accès aux images du conteneur .

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	Configuration réseau « <i>CONFIGURATION_DETAILS</i> » manquante pour les tâches dans TaskDefinition - ' <i>TASK_DEFINITION</i> '	Des problèmes de configuration réseau peuvent survenir en raison d'une configuration VPC manquante ou de sous-réseaux manquants ou vides. Vérifiez que la configuration de votre réseau est correcte. Pour plus d'informations, consultez Conditions préalables à l'accès aux images du conteneur . Pour plus d'informations, consultez les paramètres de définition des tâches Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.
	Les tâches démarrées lorsque les clusters étaient dotés d'une balise d'exclusion sont exclues de la surveillance du temps d'exécution. Identifiant (s) de tâche concerné (s) : ' <i>TASK_ID</i> '	Lorsque vous modifiez la GuardDuty balise prédéfinie de GuardDutyManaged - true à GuardDutyManaged - false, il ne GuardDuty recevra pas les événements d'exécution pour ce cluster Amazon ECS. Mettez à jour le tag sur GuardDutyManaged -, true puis relancez la tâche.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	Les services déployés lorsque les clusters étaient dotés d'une balise d'exclusion sont exclus de la surveillance du temps d'exécution. Nom (s) du service concerné : « <i>SERVICE_NAME</i> »	Lorsque les services sont déployés avec la balise d'exclusion GuardDuty Managed -false, ils ne GuardDuty recevront pas d'événements d'exécution pour ce cluster Amazon ECS. Mettez à jour le tag sur GuardDutyManaged -, true puis redéployez le service.
	Les tâches démarrées avant l'activation de la configuration automatisée des agents ne sont pas couvertes. Identifiant (s) des tâches concernées : « <i>TASK_ID</i> »	Lorsque le cluster contient une tâche lancée avant d'activer la configuration de l'agent automatisé pour Amazon ECS, il ne GuardDuty sera pas en mesure de la protéger. Relancez la tâche pour qu'elle soit surveillée par GuardDuty
	Les services déployés avant l'activation de la configuration automatisée des agents ne sont pas couverts. Nom (s) du service concerné : « <i>SERVICE_NAME</i> »	Lorsque les services sont déployés avant d'activer la configuration automatisée des agents pour Amazon ECS, GuardDuty aucun événement d'exécution n'est reçu pour les clusters ECS.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	<p>Le service <i>SERVICE_NAME</i> « » nécessite un nouveau déploiement pour fix/troubleshoot. Reportez-vous à la documentation, Nom (s) du service concerné : « <i>SERVICE_NAME</i> »</p>	<p>Un service démarré avant l'activation de la surveillance du temps d'exécution n'est pas pris en charge.</p> <p>Vous pouvez soit redémarrer le service, soit le mettre à jour avec l'option <code>forceNewDeployment</code> en suivant les étapes décrites dans la section Mettre à jour un service Amazon ECS à l'aide de la console dans le manuel Amazon Elastic Container Service Developer Guide. Vous pouvez également suivre les étapes ci-dessous UpdateServices dans le manuel Amazon Elastic Container Service API Reference.</p>
	<p>Les tâches démarrées avant l'activation de la surveillance du temps d'exécution doivent être relancées. Identifiant (s) des tâches concernées : « <i>TASK_ID_1</i> »</p>	<p>Dans Amazon ECS, les tâches sont immuables. Pour évaluer le comportement d'exécution ou une AWS Fargate tâche en cours d'exécution, assurez-vous que la surveillance du temps d'exécution est déjà activée, puis redémarrez la tâche GuardDuty pour ajouter le sidecar du conteneur.</p>

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
Autres	<p>Problème non identifié, pour les tâches dans TaskDefinition - ' <i>TASK_DEFINITION</i> '</p>	<p>Utilisez les questions suivantes pour identifier la cause première du problème :</p> <ul style="list-style-type: none"> • La tâche a-t-elle démarré avant que vous n'activiez le Runtime Monitoring ? <p>Dans Amazon ECS, les tâches sont immuables. Pour évaluer le comportement d'exécution d'une tâche Fargate en cours d'exécution, assurez-vous que la surveillance du temps d'exécution est déjà activée, puis redémarrez la tâche GuardDuty pour ajouter le sidecar du conteneur.</p> <ul style="list-style-type: none"> • Cette tâche fait-elle partie d'un déploiement de service qui a débuté avant que vous n'activiez le Runtime Monitoring ? <p>Dans l'affirmative, vous pouvez redémarrer le service ou le mettre à jour <code>forceNewDeployment</code> en suivant les étapes décrites dans la section Mettre à jour un service.</p>

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
		<p>Vous pouvez également utiliser UpdateService ou AWS CLI.</p> <ul style="list-style-type: none">• La tâche a-t-elle été lancée après avoir exclu le cluster ECS de la surveillance du temps d'exécution ? <p>Lorsque vous modifiez la GuardDuty balise prédéfinie de GuardDutyManaged - true à GuardDutyManaged - false, il ne GuardDuty recevra pas les événements d'exécution pour le cluster ECS.</p> <ul style="list-style-type: none">• Votre service contient-il une tâche dont l'ancien format est taskArn ? <p>GuardDuty Runtime Monitoring ne prend pas en charge la couverture des tâches dont l'ancien format est taskArn.</p> <p>Pour plus d'informations sur les Amazon Resource Names (ARN) pour les ressources Amazon ECS, consultez Amazon Resource Names (ARN) and IDs.</p>

Couverture du temps d'exécution et résolution des problèmes pour les clusters Amazon EKS

Après avoir activé la surveillance du temps d'exécution et installé l'agent de GuardDuty sécurité (module complémentaire) pour EKS manuellement ou par le biais d'une configuration automatique de l'agent, vous pouvez commencer à évaluer la couverture de vos clusters EKS.

Table des matières

- [Consultation des statistiques de couverture](#)
- [Modification de l'état de couverture avec EventBridge notifications](#)
- [Résolution des problèmes de couverture du temps d'exécution d'Amazon EKS](#)

Consultation des statistiques de couverture

Les statistiques de couverture pour les clusters EKS associés à vos propres comptes ou à vos comptes membres sont le pourcentage de clusters EKS sains par rapport à tous les clusters EKS de la Région AWS sélectionnée. L'équation suivante représente cela comme suit :

$$(\text{clusters/All Clusters sains}) * 100$$

Choisissez l'une des méthodes d'accès pour consulter les statistiques de couverture de vos comptes.

Console

- Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
- Dans le volet de navigation, choisissez Runtime Monitoring.
- Choisissez l'onglet Couverture d'exécution du cluster EKS.
- Dans l'onglet Couverture d'exécution du cluster EKS, vous pouvez consulter les statistiques de couverture agrégées selon l'état de couverture disponible dans le tableau Liste des clusters.
 - Vous pouvez filtrer le tableau Liste des clusters selon les colonnes suivantes :
 - Nom du cluster
 - ID de compte
 - Type de gestion des agents
 - État de couverture

- Add-on Version
- Si l'un de vos clusters EKS a un état de couverture Non sain, la colonne Problème peut inclure des informations supplémentaires sur la raison de l'état Défectueux.

API/CLI

- Exécutez l'[ListCoverage](#) API avec votre propre identifiant de détecteur, votre région et votre point de terminaison de service valides. Vous pouvez filtrer et trier la liste des clusters à l'aide de cette API.
- Vous pouvez modifier l'exemple de `filter-criteria` à l'aide de l'une des options suivantes pour `CriterionKey` :
 - ACCOUNT_ID
 - CLUSTER_NAME
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - ADDON_VERSION
 - MANAGEMENT_TYPE
- Vous pouvez modifier l'exemple de `AttributeName` dans `sort-criteria` à l'aide des options suivantes :
 - ACCOUNT_ID
 - CLUSTER_NAME
 - COVERAGE_STATUS
 - ISSUE
 - ADDON_VERSION
 - UPDATED_AT
- Vous pouvez modifier le *max-results* (jusqu'à 50).
- `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
```

```
'{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}]}] }' --max-results 5
```

- Exécutez l'[GetCoverageStatistics](#) API pour récupérer les statistiques agrégées de couverture sur la base de `statisticsType`.
- Vous pouvez modifier l'exemple de `statisticsType` sur l'une des options suivantes :
 - `COUNT_BY_COVERAGE_STATUS` : représente les statistiques de couverture pour les clusters EKS agrégées par état de couverture.
 - `COUNT_BY_RESOURCE_TYPE`— Statistiques de couverture agrégées en fonction du type de AWS ressource figurant dans la liste.
- Vous pouvez modifier l'exemple de `filter-criteria` dans la commande. Vous pouvez utiliser les options suivantes pour `CriterionKey` :
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `ADDON_VERSION`
 - `MANAGEMENT_TYPE`
- `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id
12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
"FilterCondition":{"EqualsValue":"123456789012"}]}] }'
```

Si l'état de couverture de votre cluster EKS est Défectueux, veuillez consulter [Résolution des problèmes de couverture du temps d'exécution d'Amazon EKS](#).

Modification de l'état de couverture avec EventBridge notifications

L'état de couverture d'un cluster EKS sur votre compte peut être indiqué comme étant Défectueux. Pour détecter les cas où l'état de couverture devient Défectueux, nous vous recommandons de surveiller régulièrement l'état de couverture et de résoudre les problèmes, si l'état est Défectueux

Vous pouvez également créer une EventBridge règle Amazon pour vous avertir lorsque le statut de couverture passe de Healthy ou non Unhealthy à. Par défaut, il le GuardDuty publie dans le [EventBridge bus](#) pour votre compte.

Exemple de schéma de notification

Dans une EventBridge règle, vous pouvez utiliser les exemples d'événements et de modèles d'événements prédéfinis pour recevoir une notification de l'état de couverture. Pour plus d'informations sur la création d'une EventBridge règle, consultez la section [Créer une règle](#) dans le guide de EventBridge l'utilisateur Amazon.

En outre, vous pouvez créer un modèle d'événement personnalisé à l'aide de l'exemple de schéma de notification suivant. Assurez-vous de remplacer les valeurs de votre compte. Pour être averti lorsque le statut de couverture de votre cluster Amazon EKS passe de Healthy à Unhealthy, le detail-type doit être *GuardDuty Runtime Protection Unhealthy*. Pour être averti lorsque le statut de couverture passe de Unhealthy à Healthy, remplacez la valeur de detail-type par *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Compte AWS ID",
  "time": "event timestamp (string)",
  "region": "Région AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EKS",
      "eksClusterDetails": {
        "clusterName": "string",
        "availableNodes": "string",
        "desiredNodes": "string",
        "addonVersion": "string"
      }
    }
  },
}
```

```

    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Résolution des problèmes de couverture du temps d'exécution d'Amazon EKS

Si l'état de couverture de votre cluster EKS est le suivant `Unhealthy`, vous pouvez afficher l'erreur correspondante soit dans la colonne Problème de la GuardDuty console, soit en utilisant le type de [CoverageResource](#) données.

Lorsque vous utilisez des balises d'inclusion ou d'exclusion pour surveiller vos clusters EKS de manière sélective, la synchronisation des balises peut prendre un certain temps. Cela peut avoir un impact sur l'état de couverture du cluster EKS associé. Vous pouvez réessayer de supprimer et d'ajouter la balise correspondante (inclusion ou exclusion). Pour plus d'informations, veuillez consulter [Étiquetage de vos ressources Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS.

La structure d'un problème de couverture est `Issue type:Extra information`. Généralement, les problèmes comportent des informations supplémentaires facultatives qui peuvent inclure une exception spécifique côté client ou une description du problème. Sur la base d'informations supplémentaires, les tableaux suivants fournissent les étapes recommandées pour résoudre les problèmes de couverture de vos clusters EKS.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
La création de l'addon a échoué	L'addon <code>aws-guardduty-agent</code> est pas compatible avec la version actuelle du cluster <code>ClusterName</code> . Le module complémentaire spécifié n'est pas pris en charge.	Assurez-vous que vous utilisez l'une de ces versions de Kubernetes prenant en charge le déploiement du module complémentaire EKS <code>aws-guardduty-agent</code> . Pour plus d'informations, consultez Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty . Pour plus d'informations sur la mise

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
		à jour de votre version de Kubernetes, veuillez consulter la section Mise à jour d'une version Kubernetes de cluster Amazon EKS .
<p>La création de l'addon a échoué</p> <p>La mise à jour de l'extension a échoué</p> <p>État de l'addon malsain</p>	<p>Problème de module complémentaire EKS :</p> <p>AddonIssueCode :</p> <p>AddonIssueMessage</p>	<p>Pour plus d'informations sur les étapes recommandées pour un code de problème spécifique à un module complémentaire, consultez Troubleshooting steps for Addon creation/update error with Addon issue code.</p> <p>Pour obtenir la liste des codes d'erreur liés aux modules complémentaires que vous pourriez rencontrer dans le cadre de ce problème, consultez AddonIssue.</p>
Échec de la création du point de terminaison VPC	La création de points de terminaison VPC n'est pas prise en charge pour les VPC partagés <i>vpcId</i>	<p>Runtime Monitoring prend désormais en charge l'utilisation d'un VPC partagé au sein d'une organisation. Assurez-vous que vos comptes répondent à toutes les conditions requises. Pour plus d'informations, consultez Conditions préalables à l'utilisation d'un VPC partagé.</p>

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
	<p>Uniquement lors de l'utilisation d'un VPC partagé avec configuration d'agent automatisée</p> <p>L'ID 111122223333 de compte propriétaire du VPC partagé vpcId n'est activé ni sur la surveillance du temps d'exécution, ni sur la configuration automatique des agents, ni sur les deux.</p> <p>L'activation du DNS privé nécessite à la fois que <code>enableDnsSupport</code> les attributs <code>enableDnsHostnames</code> VPC soient définis sur <code>true</code> for vpcId (Service : Ec2, Status Code:400, Request ID :). a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</p>	<p>Le compte propriétaire du VPC partagé doit activer la surveillance du temps d'exécution et la configuration automatique des agents pour au moins un type de ressource (Amazon EKS ou Amazon ECS (AWS Fargate)) . Pour plus d'informations, consultez Prérequis spécifiques à la surveillance du temps d' GuardDuty exécution.</p> <p>Assurez-vous que les attributs de VPC suivants sont définis sur <code>true</code> : <code>enableDnsSupport</code> et <code>enableDnsHostnames</code> . Pour plus d'informations, veuillez consulter la rubrique Attributs DNS dans votre VPC.</p> <p>Si vous utilisez la console Amazon VPC https://console.aws.amazon.com/vpc/ pour créer l'Amazon VPC, assurez-vous de sélectionner à la fois Activer les noms d'hôte DNS et Activer la résolution DNS. Pour plus d'informations, veuillez consulter Options de configuration de VPC.</p>

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
La suppression du point de terminaison VPC partagé a échoué	La suppression du point de terminaison VPC partagé n'est pas autorisée pour l'ID de compte 111122223333 , le VPC vpcId partagé et l'ID de compte propriétaire. 555555555555	<p>Étapes potentielles :</p> <ul style="list-style-type: none"> La désactivation de l'état de surveillance du temps d'exécution du compte de participant VPC partagé n'a aucun impact sur la politique de point de terminaison du VPC partagé ni sur le groupe de sécurité existant dans le compte propriétaire. <p>Pour supprimer le point de terminaison et le groupe de sécurité VPC partagés, vous devez désactiver la surveillance du temps d'exécution ou l'état de configuration automatique de l'agent dans le compte propriétaire du VPC partagé.</p> <ul style="list-style-type: none"> Le compte de participant VPC partagé ne peut pas supprimer le point de terminaison et le groupe de sécurité VPC partagés hébergés dans le compte propriétaire du VPC partagé.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Clusters EKS locaux	Les modules complémentaires EKS ne sont pas prises en charge sur les clusters Outpost locaux.	Non exploitable. Pour plus d'informations, consultez Amazon EKS sur les AWS avant-postes .
Autorisation d'activation de la surveillance d'exécution EKS non accordée	(peut afficher ou non des informations supplémentaires)	<ol style="list-style-type: none"> 1. Si des informations supplémentaires sont disponibles pour ce problème, corrigez la cause première et passez à l'étape suivante. 2. Activez la surveillance d'exécution EKS pour la désactiver, puis la réactiver. Assurez-vous que l' GuardDutyagent est également déployé, que ce soit automatiquement GuardDuty ou manuellement.
la surveillance d'exécution EKS permet l'allocation de ressources en cours	(peut afficher ou non des informations supplémentaires)	Non exploitable. Une fois que vous avez activé la surveillance d'exécution EKS, l'état de couverture peut rester <code>Unhealthy</code> jusqu'à la fin de l'étape d'allocation des ressources. L'état de couverture est surveillé et mis à jour périodiquement.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Autres (tout autre problème)	Erreur due à un échec d'autorisation	Activez la surveillance d'exécution EKS pour la désactiver, puis la réactiver. Assurez-vous que l' GuardDuty agent est également déployé, automatiquement GuardDuty ou manuellement.

Étapes de résolution d'une creation/update erreur d'addon avec le code de problème de l'addon

	Étapes de résolution des problèmes
Erreur de création ou de mise à jour de l'addon	
Problème lié à l'addon EKS - <code>InsufficientNumberReplicas</code> : Le module complémentaire est défectueux car il ne contient pas le nombre de répliques souhaité.	<ul style="list-style-type: none"> À l'aide du message du problème, vous pouvez identifier et corriger la cause première. Vous pouvez commencer par décrire votre cluster. Par exemple, kubectl describe pods à utiliser pour identifier la cause première de la défaillance du pod. <p>Après avoir corrigé la cause première, réessayez l'étape (création ou mise à jour d'un module complémentaire).</p> <ul style="list-style-type: none"> Si le problème persiste, vérifiez que le point de terminaison VPC de votre cluster Amazon EKS est correctement configuré. Pour plus d'informations, consultez Validation de la configuration des points de terminaison VPC.
Problème lié à l'addon EKS - <code>InsufficientNumberReplicas</code> : Le module complémentaire n'est pas sain car un ou	Pour résoudre ce problème, vous pouvez procéder de l'une des manières suivantes :

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
<p>plusieurs pods ne sont pas planifiés. Des 0/x nœuds sont disponibles :x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never .</p>	<ul style="list-style-type: none"> • Mettez à jour la priorité du pod de l' GuardDuty agent : Paramètres et valeurs configurables en PriorityClass affectant à l'une des options prenant en charge la preemptionPolicy valeur commePreemptLowerPriority . Pour plus d'informations sur la priorité des pods, consultez la section Priorité et préemption des pods dans la documentation de Kubernetes. • Élargissez l'instance : pour gérer vos ressources et sélectionner une instance optimale, consultez Gérer les ressources de calcul à l'aide de nœuds et Choisir un type d'instance de nœud Amazon EC2 optimal dans le guide de l'utilisateur Amazon EKS.
<p>Problème lié à l'addon EKS - InsufficientNumberOfReplicas : Le module complémentaire n'est pas sain car un ou plusieurs pods ne sont pas planifiés. Des 0/x nœuds sont disponibles :x Too many pods. preemption: not eligible due to preemptionPolicy=Never .</p>	
<p>Problème lié à l'addon EKS - InsufficientNumberOfReplicas : Le module complémentaire n'est pas sain car un ou plusieurs pods ne sont pas planifiés. Des 0/x nœuds sont disponibles :1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never .</p>	

 Note

Le message s'affiche 0/x car seule la première erreur détectée est GuardDuty signalée. Le nombre réel de pods en cours d'exécution dans le GuardDuty daemonset peut être supérieur à 0.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
<p>Problème lié à l'extension EKS - <code>InsufficientNumberOfReplicas</code> : L'extension n'est pas saine car un ou plusieurs pods contiennent des conteneurs en attente <code>CrashLoopBackOff: Completed</code></p>	<p>Vous pouvez consulter les journaux associés au module et identifier le problème. Pour plus d'informations sur la procédure à suivre, consultez la section Debug Running Pods dans la documentation de Kubernetes.</p> <p>Utilisez la liste de contrôle suivante pour résoudre ce problème lié au module complémentaire :</p> <ul style="list-style-type: none">• Vérifiez que la surveillance du temps d'exécution est activée.• Vérifiez que les conditions Conditions préalables à la prise en charge des clusters Amazon EKS, telles que les distributions de système d'exploitation vérifiées et les versions de Kubernetes prises en charge, sont respectées.• Lorsque vous gérez l'agent de sécurité manuellement, vérifiez que vous avez créé un point de terminaison VPC pour tous les VPC. Lorsque vous activez la configuration GuardDuty automatique, vous devez toujours vérifier que le point de terminaison VPC est créé. Par exemple, lors de l'utilisation d'un VPC partagé dans une configuration automatisée. <p>Pour valider cela, consultez Validation de la configuration des points de terminaison VPC.</p> <ul style="list-style-type: none">• Vérifiez que l'agent GuardDuty de sécurité est capable de résoudre le DNS privé du point de terminaison GuardDuty VPC.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
	<p>Pour connaître les points de terminaison, consultez la section Noms DNS privés des points de terminaison dans. Gestion des agents GuardDuty de sécurité</p> <p>Pour ce faire, vous pouvez utiliser nslookup un outil sous Windows ou Mac, ou dig un outil sous Linux. Lorsque vous utilisez nslookup, vous pouvez utiliser la commande suivante après avoir remplacé la région <i>us-west-2</i> par votre région :</p> <div data-bbox="862 825 1507 945"><pre>nslookup guardduty-data. <i>us-west-2</i>.amazonaws.com</pre></div> <ul style="list-style-type: none">• Vérifiez que votre politique de point de terminaison GuardDuty VPC ou la politique de contrôle des services n'ont aucune incidence sur guardduty:SendSecurityTelemetry l'action.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
<p>Problème lié à l'extension EKS - InsufficientNumberOfReplicas : L'extension n'est pas saine car un ou plusieurs pods contiennent des conteneurs en attente</p> <p>CrashLoopBackOff: Error</p>	<p>Vous pouvez consulter les journaux associés au module et identifier le problème. Pour plus d'informations sur la procédure à suivre, consultez la section Debug Running Pods dans la documentation de Kubernetes.</p> <p>Après avoir identifié le problème, utilisez la liste de contrôle suivante pour le résoudre :</p> <ul style="list-style-type: none"> • Vérifiez que la surveillance du temps d'exécution est activée. • Vérifiez que les conditions Conditions préalables à la prise en charge des clusters Amazon EKS, telles que les distributions de système d'exploitation vérifiées et les versions de Kubernetes prises en charge, sont respectées. • L'agent GuardDuty de sécurité est capable de résoudre le DNS privé du point de terminaison du GuardDuty VPC. Pour connaître les points de terminaison, consultez la section Noms DNS privés des points de terminaison dans. Gestion des agents GuardDuty de sécurité
<p>Problème lié à l'addon EKS - Admission RequestDenied : le webhook d'admission "validate.kyverno.svc-fail" a refusé la demande : politique de violation DaemonSet/amazon-guardduty/aws-guardduty-agent des ressources : restrict-image-registries : ... autogen-validate-registries</p>	<ol style="list-style-type: none"> 1. Le cluster Amazon EKS ou l'administrateur de sécurité doivent revoir la politique de sécurité qui bloque la mise à jour de l'addon. 2. Vous devez soit désactiver le contrôleur (webhook), soit lui demander d'accepter les demandes d'Amazon EKS.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
<p>Problème lié à l'extension EKS - ConfigurationConflict : Conflits détectés lors de la tentative de candidature. Ne continuer a pas en raison du mode de résolution des conflits. Conflicts: DaemonSet.apps.aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image</p>	<p>Lors de la création ou de la mise à jour de l'addon, fournissez l'indicateur de OVERWRITE résolution des conflits. Cela remplacer a potentiellement toutes les modifications apportées directement aux ressources associées dans Kubernetes à l'aide de l'API Kubernetes.</p> <p>Vous pouvez d'abord supprimer un module complémentaire Amazon EKS d'un cluster, puis le réinstaller.</p>

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
<p>Problème lié à l'extension EKS - AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope</p> <p>AddonUpdationFailed: EKSAaddonIssue - AccessDenied: namespaces\"amazon-guardduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guardduty\"</p>	<p>Vous devez ajouter eks:addon-cluster-admin ClusterRoleBinding manuellement l'autorisation manquante. Ajoutez ce qui suit yaml à eks:addon-cluster-admin :</p> <pre>--- kind: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/v1 metadata: name: eks:addon-cluster-admin subjects: - kind: User name: eks:addon-manager apiGroup: rbac.authorization.k8s.io roleRef: kind: ClusterRole name: cluster-admin apiGroup: rbac.authorization.k8s.io ---</pre> <p>Vous pouvez désormais l'appliquer yaml à votre cluster Amazon EKS à l'aide de la commande suivante :</p> <pre>kubectl apply -f eks-addon-cluster-admin.yaml</pre>

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
<p>Problème lié à l'extension EKS - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label</p>	<p>Vous devez soit désactiver le contrôleur, soit lui demander d'accepter les demandes du cluster Amazon EKS.</p> <p>Avant de créer ou de mettre à jour le module complémentaire, vous pouvez également créer un espace de GuardDuty noms et l'étiqueter comme owner suit.</p>
<p>Problème lié à l'extension EKS - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container-registries] container <aws-guardduty-agent> has an invalid image registry</p>	<p>Ajoutez le registre d'images GuardDuty pour allowed-container-registries dans votre contrôleur d'admission. Pour plus d'informations, consultez le référentiel ECR pour EKS v1.8.1-eks-build.2 dans. Agent d'hébergement GuardDuty de référentiels Amazon ECR</p>

Configuration de la surveillance du processeur et de la mémoire

Après avoir activé la surveillance du temps d'exécution et vérifié que l'état de couverture de votre cluster est sain, vous pouvez configurer et consulter les indicateurs d'analyse.

Les rubriques suivantes peuvent vous aider à évaluer les performances de l'agent déployé par rapport aux limites de processeur et de mémoire de l' GuardDuty agent.

Configuration de la surveillance sur le cluster Amazon ECS

Les étapes suivantes du guide de l' CloudWatch utilisateur Amazon peuvent vous aider à évaluer les performances de l'agent déployé par rapport aux limites de processeur et de mémoire de l' GuardDuty agent :

1. [Configuration de Container Insights sur Amazon ECS pour les métriques relatives aux clusters et aux niveaux de service](#)
2. [Statistiques d'Amazon ECS Container Insights](#)

Configuration de la surveillance sur le cluster Amazon EKS

Une fois que l'agent de GuardDuty sécurité a été déployé et que vous avez déterminé que l'état de couverture de votre cluster est sain, vous pouvez configurer et consulter les métriques de Container Insights.

Évaluer les performances de l'agent de sécurité

1. [Configuration de Container Insights sur Amazon EKS et Kubernetes dans le guide](#) de l'utilisateur Amazon CloudWatch
2. [Statistiques Amazon EKS et Kubernetes Container Insights dans le guide de](#) l'utilisateur Amazon CloudWatch

Gérez les performances avec l'agent de sécurité v1.5.0 et versions ultérieures

Avec l'agent de sécurité [v1.5.0 et versions ultérieures](#), lorsque les informations indiquent que l'GuardDuty agent associé atteint les limites assignées, vous pouvez configurer des paramètres spécifiques. Pour plus d'informations, consultez [Configuration des paramètres du module complémentaire EKS](#).

Utilisation d'un VPC partagé avec surveillance du temps d'exécution

GuardDuty La surveillance du temps d'exécution prend en charge l'utilisation d'Amazon Virtual Private Cloud (Amazon VPC) partagé pour ceux Comptes AWS qui appartiennent à la même organisation dans. AWS Organizations Vous pouvez utiliser le VPC partagé de deux manières :

- Configuration automatique de l'agent (recommandée) — Lorsque l'agent de sécurité est GuardDuty automatiquement géré, il configure également la politique de point de terminaison Amazon VPC. Cette politique est basée sur les paramètres VPC partagés de votre organisation.

Vous devez activer la configuration automatique des agents dans le compte propriétaire du VPC partagé et dans tous les comptes participants qui partageront ce VPC.

- Agent géré manuellement : lorsque vous gérez manuellement l'agent de sécurité avec un VPC partagé, vous devez mettre à jour la politique de point de terminaison du VPC pour autoriser les comptes correspondants à accéder au VPC partagé. Pour ce faire, vous pouvez utiliser l'exemple de politique présenté dans la [Comment ça marche](#) section suivante.

Pour les scénarios de gestion manuelle impliquant des comptes participants pour un VPC partagé, l'état de couverture peut ne pas être précis. Pour garantir la protection et l'état de couverture à jour de vos ressources, il est GuardDuty recommandé d'activer la configuration automatique des agents pour tous les comptes qui utiliseront un VPC partagé.

Rubriques

- [Comment ça marche](#)
- [Conditions préalables à l'utilisation d'un VPC partagé](#)

Comment ça marche

Ceux Comptes AWS qui appartiennent à la même organisation que le compte propriétaire Amazon VPC partagé peuvent également partager le même point de terminaison Amazon VPC. Chacun des comptes qui partagent le même Amazon VPC est appelé AWS compte de participant du Amazon VPC partagé associé.

L'exemple suivant montre la politique de point de terminaison VPC par défaut du compte propriétaire du VPC partagé et du compte participant. Le `aws:PrincipalOrgID` affichera l'ID d'organisation associé à la ressource VPC partagée. L'utilisation de cette politique est limitée aux comptes de participants présents dans l'organisation du compte propriétaire.

Exemple Exemple de politique de point de terminaison VPC partagé

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "*",
    "Resource": "*",
    "Effect": "Allow",
    "Principal": "*"
  },
  {
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalOrgID": "o-abcdef0123"
      }
    }
  }
]
```

```
    }  
  },  
  "Action": "*",  
  "Resource": "*",  
  "Effect": "Deny",  
  "Principal": "*" }  
]  
}
```

Avec configuration GuardDuty automatique de l'agent

Lorsque le compte propriétaire du VPC partagé active la surveillance du temps d'exécution et la configuration automatisée des agents pour l'une des ressources (Amazon EKS ou (AWS Fargate Amazon ECS uniquement)), tous les VPC partagés sont éligibles à l'installation automatique du point de terminaison Amazon VPC partagé et du groupe de sécurité associé dans le compte propriétaire du VPC partagé. GuardDuty récupère l'ID d'organisation associé à l'Amazon VPC partagé.

GuardDuty crée un point de terminaison Amazon VPC lorsque le compte propriétaire du VPC partagé ou le compte participant en a besoin. Parmi les exemples de besoin d'un point de terminaison Amazon VPC, citons l'activation GuardDuty, la surveillance du temps d'exécution, la surveillance du temps d'exécution EKS ou le lancement d'une nouvelle tâche Amazon ECS-Fargate . Lorsque ces comptes activent la surveillance du temps d'exécution et la configuration automatique des agents pour n'importe quel type de ressource, ils GuardDuty créent un point de terminaison Amazon VPC et définissent la politique du point de terminaison avec le même identifiant d'organisation que celui du compte propriétaire du VPC partagé. GuardDuty ajoute une GuardDutyManaged balise et lui attribue la valeur `true` pour le point de terminaison Amazon VPC qui GuardDuty le crée. Si le compte propriétaire Amazon VPC partagé n'a pas activé la surveillance du temps d'exécution ou la configuration automatique des agents pour aucune des ressources, il ne GuardDuty définira pas la politique relative aux points de terminaison Amazon VPC. Pour plus d'informations sur la configuration de la surveillance du temps d'exécution et la gestion automatique de l'agent de sécurité dans le compte propriétaire du VPC partagé, consultez [Activer la surveillance du GuardDuty temps d'exécution](#)

Utilisation avec un agent géré manuellement

Lorsque vous utilisez un VPC partagé avec un agent géré manuellement, vérifiez qu'aucune politique de point de Deny terminaison explicite ne bloque les comptes devant utiliser le VPC partagé. Cela empêche l'agent de sécurité d'envoyer des données télémétriques à GuardDuty, ce qui se

traduit par un état de Unhealthy couverture. Pour configurer la politique relative aux terminaux, consultez [Exemple shared VPC endpoint policy](#).

La couverture du temps d'exécution peut ne pas être précise dans des scénarios tels que l'absence d'autorisations sur le VPC partagé. Vous pouvez surveiller en permanence la couverture des ressources en suivant les étapes correspondant à votre type de ressource dans [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#).

Pour garantir la protection continue de vos ressources informatiques par le biais de la surveillance du temps d'exécution, il est GuardDuty recommandé d'activer la configuration automatique des agents pour le compte propriétaire du VPC partagé et pour tous les comptes participants associés à vos ressources.

Conditions préalables à l'utilisation d'un VPC partagé

Dans le cadre de la configuration initiale, effectuez les Compte AWS étapes suivantes si vous souhaitez devenir propriétaire du VPC partagé :

1. Création d'une organisation : créez une organisation en suivant les étapes décrites dans la [section Création et gestion d'une organisation](#) du Guide de AWS Organizations l'utilisateur.

Pour plus d'informations sur l'ajout ou la suppression de comptes de membres, consultez [la section Gestion Comptes AWS au sein de votre organisation](#).

2. Création d'une ressource VPC partagée — Vous pouvez créer une ressource VPC partagée à partir du compte du propriétaire. Pour plus d'informations, consultez [Partager vos sous-réseaux VPC avec d'autres comptes](#) dans le guide de l'utilisateur Amazon VPC.

Prérequis spécifiques à la surveillance du temps d' GuardDuty exécution

La liste suivante fournit les prérequis spécifiques à GuardDuty :

- Le compte propriétaire du VPC partagé et le compte participant peuvent provenir de différentes organisations de. GuardDuty Cependant, ils doivent appartenir à la même organisation que AWS Organizations. Cela est nécessaire pour GuardDuty créer un point de terminaison Amazon VPC et un groupe de sécurité pour le VPC partagé. Pour plus d'informations sur le fonctionnement des VPC partagés, consultez [Partager votre VPC avec d'autres](#) comptes dans le guide de l'utilisateur Amazon VPC.
- Activez la surveillance du temps d'exécution ou la surveillance du temps d'exécution EKS, ainsi que la configuration GuardDuty automatique des agents pour toutes les ressources du compte

propriétaire du VPC partagé et du compte participant. Pour plus d'informations, consultez [Activer la surveillance du temps d'exécution](#).

Si vous avez déjà effectué ces configurations, passez à l'étape suivante.

- Lorsque vous travaillez avec une tâche Amazon EKS ou Amazon ECS (AWS Fargate uniquement), assurez-vous de choisir la ressource VPC partagée associée au compte propriétaire et de sélectionner ses sous-réseaux.

Utilisation de l'infrastructure en tant que code (IaC) avec des agents de sécurité GuardDuty automatisés

Utilisez cette section uniquement si la liste suivante s'applique à votre cas d'utilisation :

- Vous utilisez des outils d'infrastructure en tant que code (IaC), tels que Terraform, pour gérer vos AWS ressources, Cloud Development Kit AWS (AWS CDK) et
- Vous devez activer la configuration GuardDuty automatique des agents pour un ou plusieurs types de ressources : Amazon EKS, Amazon EC2 ou Amazon. ECS-Fargate

Présentation du graphe de dépendance des ressources IaC

Lorsque vous activez la configuration GuardDuty automatique de l'agent pour un type de ressource, vous GuardDuty créez automatiquement un point de terminaison VPC et un groupe de sécurité associés à ce point de terminaison VPC, puis installez l'agent de sécurité pour ce type de ressource. Par défaut, le point de terminaison VPC et le groupe de sécurité associé ne GuardDuty seront supprimés qu'après avoir désactivé la surveillance du temps d'exécution. Pour plus d'informations, consultez [Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring](#).

Lorsque vous utilisez un outil IaC, celui-ci gère un graphe de dépendance des ressources. Au moment de la suppression de ressources à l'aide de l'outil IaC, celui-ci supprime uniquement les ressources qui peuvent être suivies dans le cadre du graphe de dépendance des ressources. Les outils IaC peuvent ne pas connaître les ressources créées en dehors de leur configuration spécifiée. Par exemple, vous créez un VPC avec un outil IaC, puis vous ajoutez un groupe de sécurité à ce VPC à l'aide d'une AWS console ou d'une opération d'API. Dans le graphe de dépendance des ressources, la ressource VPC que vous créez dépend du groupe de sécurité associé. Si vous supprimez cette ressource VPC à l'aide de l'outil IaC, vous obtiendrez une erreur. Le moyen de

contourner cette erreur consiste à supprimer manuellement le groupe de sécurité associé ou à mettre à jour la configuration laC pour inclure cette ressource ajoutée.

Problème courant : suppression de ressources dans laC

Lorsque vous utilisez la configuration GuardDuty automatique des agents, vous souhaitez peut-être supprimer une ressource (Amazon EKS, Amazon EC2 ou Amazon ECS-Fargate) que vous avez créée à l'aide d'un outil laC. Toutefois, cette ressource dépend d'un point de terminaison VPC créé. GuardDuty Cela empêche l'outil laC de supprimer la ressource par lui-même et vous oblige à désactiver la surveillance du temps d'exécution, qui supprime automatiquement le point de terminaison VPC.

Par exemple, lorsque vous tentez de supprimer le point de terminaison VPC GuardDuty créé en votre nom, une erreur similaire aux exemples suivants s'affiche.

Exemple

Exemple d'erreur lors de l'utilisation du CDK

The following resource(s) failed to delete:

```
[mycdkvpapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
HandlerErrorCode: InvalidRequest)
```

Exemple

Exemple d'erreur lors de l'utilisation de Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
20m0s elapsed]
```

```
Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

 Note

Le AWS fournisseur Terraform version 6.43.0 et versions ultérieures résout automatiquement ce problème. Le AWS fournisseur détecte et supprime les points de terminaison et les groupes de sécurité GuardDuty-managed VPC pendant. `terraform destroy` Ce correctif s'applique à tous les types de ressources (Amazon EKS, Amazon EC2 et Amazon ECS-Fargate).

Solution - Empêcher le problème de suppression de ressources

Cette section vous aide à gérer le point de terminaison et le groupe de sécurité VPC indépendamment de. GuardDuty

Pour vous approprier totalement les ressources configurées à l'aide de l'outil iAC, effectuez les étapes suivantes dans l'ordre indiqué :

1. Créez un VPC. Pour autoriser l'entrée, associez un point de terminaison GuardDuty VPC au groupe de sécurité à ce VPC.
2. Activez la configuration GuardDuty automatique des agents pour votre type de ressource

Une fois les étapes précédentes terminées, il ne GuardDuty créera pas son propre point de terminaison VPC et réutilisera celui que vous avez créé à l'aide de l'outil IaC.

Pour plus d'informations sur la création de votre propre VPC, consultez [Créer un VPC uniquement dans les passerelles Amazon VPC](#) Transit. Pour plus d'informations sur la création d'un point de terminaison VPC, consultez la section suivante pour votre type de ressource :

- Pour Amazon EC2, consultez. [Prérequis — Création manuelle d'un point de terminaison Amazon VPC](#)
- Pour Amazon EKS, consultez [Prérequis — Création d'un point de terminaison Amazon VPC](#).

Types d'événements d'exécution collectés qui GuardDuty utilisent

L'agent GuardDuty de sécurité collecte les types d'événements suivants et les envoie au GuardDuty backend à des fins de détection et d'analyse des menaces. GuardDuty ne vous permet pas d'accéder à ces événements. S'il GuardDuty détecte une menace potentielle et en génère un [Types](#)

[de recherche liés à la surveillance du temps](#), vous pouvez consulter les détails de la découverte correspondante.

Pour plus d'informations sur l' GuardDuty utilisation des types d'événements collectés dans Runtime Monitoring, consultez [Refus d'utiliser vos données pour améliorer le service](#).

Événements de processus

Les événements de processus représentent les informations associées aux processus exécutés sur les instances Amazon EC2 et les charges de travail des conteneurs. Le tableau suivant inclut les noms de champs et les descriptions des événements de processus que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Nom du processus	Nom du processus observé.
Chemin d'accès du processus	Chemin absolu de l'exécutable du processus.
ID du processus.	ID attribué au processus par le système d'exploitation.
PID de l'espace de noms	ID du processus dans un espace de noms PID secondaire différent de l'espace de noms PID au niveau de l'hôte. Pour les processus se trouvant à l'intérieur d'un conteneur, il s'agit de l>ID de processus observé à l'intérieur du conteneur.
ID d'utilisateur du processus	ID unique de l'utilisateur qui a exécuté le processus.
UUID du processus	L'identifiant unique attribué au processus par GuardDuty.
GID du processus	ID de processus du groupe de processus.
EGID du processus	ID de groupe effectif du groupe de processus.
EUID du processus	ID utilisateur effectif du processus.

Nom de champ	Description
Nom d'utilisateur du processus	Nom d'utilisateur qui a exécuté le processus.
Heure de début du processus	L'heure de création du processus. Ce champ est au format de chaîne de date UTC (2023-03-22T19:37:20.168Z).
Exécutable du processus SHA-256	Hachage SHA256 de l'exécutable du processus .
Chemin du script de processus	Chemin du fichier de script qui a été exécuté.
Variable d'environnement de processus	Variable d'environnement mise à la disposition du processus. Seuls LD_PRELOAD et LD_LIBRARY_PATH sont collectés.
Process Present Working Directory (PWD)	Référentiel de travail actuel du processus.
Processus parent	Détails de processus du processus parent. Un processus parent est un processus qui a créé le processus observé.

Nom de champ	Description
<p>Arguments de ligne de commande</p> <p>Actuellement, ce champ est limité à des versions d'agent spécifiques correspondant au type de ressource :</p> <ul style="list-style-type: none"> Fargate (Amazon ECS uniquement GuardDuty) avec agent de sécurité v1.0.0 et versions ultérieures. Instances Amazon EC2 avec agent de GuardDuty sécurité v1.0.0 et versions ultérieures. Clusters Amazon EKS avec agent de sécurité v1.4.0 et versions ultérieures. <p>Pour plus d'informations, consultez GuardDuty versions publiées de l'agent de sécurité.</p>	<p>Command-line arguments fournis au moment de l'exécution du processus. Ce champ peut contenir des données client sensibles.</p>

Événements de conteneur

Les événements relatifs aux conteneurs représentent les informations associées aux activités des charges de travail des conteneurs. Le tableau suivant inclut les noms de champs et les descriptions des événements de charge de travail du conteneur que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Nom de conteneur	<p>Nom du conteneur.</p> <p>Lorsqu'il est disponible, ce champ affiche la valeur de l'étiquette <code>io.kubernetes.container.name</code> .</p>
UID de conteneur	L'ID unique du conteneur attribué par l'environnement d'exécution du conteneur.

Nom de champ	Description
Exécution de conteneur	Exécution du conteneur (tel que <code>docker</code> ou <code>containerd</code>) utilisé pour exécuter le conteneur.
ID de l'image de conteneur	ID de l'image du conteneur.
Nom d'image de conteneur	Nom de l'image du conteneur.

AWS Fargate événements de tâches (Amazon ECS uniquement)

Fargate-Amazon Les événements de tâches ECS représentent les activités associées aux tâches Amazon ECS exécutées sur des ordinateurs Fargate. Le tableau suivant inclut les noms de champs et les descriptions des événements de ECS-Fargate tâches Amazon que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Nom de la ressource Amazon (ARN) de la tâche	L'ARN de la tâche.
Nom du cluster	Nom du cluster Amazon ECS.
Nom de famille	Le nom de famille de la définition de tâche. Le <code>family</code> est utilisé comme nom pour la définition de tâche utilisée pour lancer la tâche.
Service Name	Le nom du service Amazon ECS, si la tâche a été lancée dans le cadre d'un service.
Type de lancement	L'infrastructure sur laquelle s'exécute votre tâche. Pour la surveillance du temps d'exécution avec le type de ressource <code>asECSCluster</code> , le type de lancement peut être l'un <code>EC2</code> ou l'autre <code>FARGATE</code> .
CPU	Le nombre d'unités de processeur utilisées par la tâche, tel qu'il est indiqué dans la définition de la tâche.

Événements du pod Kubernetes

Le tableau suivant inclut les noms de champs et les descriptions des événements du pod Kubernetes que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
ID de pod	L'ID du pod Kubernetes.
Nom de pod	Nom du pod Kubernetes.
Espace de noms de pod	Nom de l'espace de noms Kubernetes auquel appartient la charge de travail Kubernetes.
Nom de cluster Kubernetes	Nom du cluster Kubernetes.

Événements du système de noms de domaine (DNS)

Les événements du système de noms de domaine (DNS) incluent les détails des requêtes DNS effectuées par vos types de ressources et les réponses correspondantes. Le tableau suivant inclut les noms de champs et les descriptions des événements DNS que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple : SOCK_RAW.
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses AF_INET est utilisée pour le protocole IPv4.
ID de direction	ID de direction de la connexion.
Numéro de protocole	Le numéro de protocole de couche 4, par exemple 17 pour UDP et 6 pour TCP.

Nom de champ	Description
IP du point de terminaison distant DNS	Adresse IP distante de la connexion.
Port du point de terminaison distant DNS	Numéro de port de la connexion.
Adresse IP du point de terminaison local du DNS	Adresse IP locale de la connexion.
Port du point de terminaison local du DNS	Numéro de port de la connexion.
Charge utile du DNS	Charge utile des paquets DNS contenant des réponses et des requêtes DNS.

Événements ouverts

Les événements ouverts sont associés à l'accès aux fichiers et à leur modification. Le tableau suivant inclut les noms de champs et les descriptions des événements ouverts que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Filepath	Chemin du fichier ouvert lors dans cet événement.
Indicateurs	Décrit le mode d'accès aux fichiers, tel que lecture seule, écriture seule et lecture-écriture.

Événement du module de charge

Le tableau suivant inclut le nom du champ et la description de l'événement du module de chargement que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Nom de module	Nom du module chargé dans le noyau.

Événements Mprotect

Les événements Mprotect fournissent des informations sur les modifications apportées aux paramètres de protection de la mémoire des processus exécutés sur les systèmes surveillés. Le tableau suivant inclut les noms de champs et les descriptions des événements Mprotect que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Plage d'adresses	Plage d'adresses pour laquelle les protections d'accès ont été modifiées.
Régions de mémoire	Spécifie la région de l'espace d'adressage d'un processus, telle que stack et heap.
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.

Événements de montage

Les événements de montage fournissent des informations associées au montage et au démontage des systèmes de fichiers sur votre ressource surveillée. Le tableau suivant inclut les noms de champs et les descriptions des événements de montage que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Cible de montage	Chemin où la source de montage est montée.
Source de montage	Chemin sur l'hôte qui est monté sur la cible de montage.
Type de système de fichiers	Représente le type de système de fichiers monté.

Nom de champ	Description
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.

Événements du lien

Les événements de liens fournissent une visibilité sur les activités de gestion des liens du système de fichiers dans vos ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements de lien que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Chemin du lien	Chemin où le lien physique est créé.
Chemin cible	Chemin du fichier vers lequel pointe le lien physique.

Événements Symlink

Les événements Symlink fournissent une visibilité sur les activités de gestion des liens symboliques du système de fichiers dans vos ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements liés aux liens symboliques que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Chemin du lien	Chemin où le lien symbolique est créé.
Chemin cible	Chemin du fichier vers lequel pointe le lien symbolique.

Événements Dup

Les événements Dup fournissent une visibilité sur la duplication des descripteurs de fichiers par les processus exécutés sur les ressources surveillées. Le tableau suivant inclut les noms de champs et

les descriptions des événements dup que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Descripteur d'ancien fichier	Descripteur de fichier qui représente un objet de fichier ouvert.
Descripteur de nouveau fichier	Descripteur de nouveau fichier dupliqué du descripteur d'ancien fichier. Aussi bien le descripteur d'un ancien fichier que celui de nouveau fichier représentent le même objet de fichier ouvert.
IP du point de terminaison distant Dup	Adresse IP distante de socket réseau représentée par le descripteur de nouveau fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.
Port du point de terminaison distant Dup	Port distant de socket réseau représenté par le descripteur de nouveau fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.
Adresse IP du point de terminaison local Dup	Adresse IP locale de socket réseau représentée par le descripteur d'ancien fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.
Port du point de terminaison local Dup	Port local de socket réseau représenté par le descripteur d'ancien fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.

Événement de mappage de mémoire

Le tableau suivant inclut le nom du champ et la description des événements de mappage de mémoire que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Filepath	Chemin du fichier auquel la mémoire est mappée.

Événements de socket

Les événements de socket fournissent des informations sur les connexions de socket réseau utilisées dans les activités des ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements de socket que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses AF_INET est utilisée pour le protocole IPv4.
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple : SOCK_RAW.
Numéro de protocole	Spécifie un protocole particulier au sein de la famille d'adresses. Il existe généralement un protocole unique dans les familles d'adresses. Par exemple, la famille d'adresses AF_INET utilise uniquement le protocole IP.

Événements de connexion

Les événements Connect fournissent une visibilité sur les connexions réseau établies par les processus sur vos ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements de connexion que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses AF_INET est utilisée pour le protocole IPv4.
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple : SOCK_RAW.

Nom de champ	Description
Numéro de protocole	Spécifie un protocole particulier au sein de la famille d'adresses. Il existe généralement un protocole unique dans les familles d'adresses. Par exemple, la famille d'adresses AF_INET utilise uniquement le protocole IP.
Filepath	Chemin du fichier socket si la famille d'adresses est AF_UNIX.
IP du point de terminaison distant	Adresse IP distante de la connexion.
Port du point de terminaison distant	Numéro de port de la connexion.
Adresse IP du point de terminaison local	Adresse IP locale de la connexion.
Port du point de terminaison local	Numéro de port de la connexion.

Événements Process VM Readv

Les événements Process VM readv fournissent une visibilité sur les opérations de lecture effectuées par les processus sur leurs propres régions de mémoire virtuelle. Le tableau suivant inclut les noms de champs et les descriptions des événements VM readv du processus que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.
PID cible	ID du processus à partir duquel la mémoire est lue.
UUID du processus cible	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Événements Process VM Writev

Les événements d'écriture des machines virtuelles de processus fournissent une visibilité sur les opérations d'écriture effectuées par les processus sur leurs propres régions de mémoire virtuelle. Le tableau suivant inclut les noms de champs et les descriptions des événements d'écriture des machines virtuelles par processus que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.
PID cible	ID du processus dans lequel la mémoire est écrite.
UUID du processus cible	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Événements de suivi des processus (Ptrace)

L'appel système Process Trace (Ptrace) est un mécanisme de débogage et de traçage qui permet à un processus (traceur) d'observer et de contrôler l'exécution d'un autre processus (cible). Cela permet au traceur d'inspecter et de modifier la mémoire, les registres et le flux d'exécution du processus cible.

Les événements Ptrace fournissent une visibilité sur l'utilisation de l'appel système ptrace par les processus exécutés sur les ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements ptrace que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
PID cible	ID du processus cible.
UUID du processus cible	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Nom de champ	Description
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.

Lier des événements

Les événements de liaison fournissent une visibilité sur la liaison des sockets réseau par les processus exécutés sur les ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements de liaison que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses AF_INET est utilisée pour le protocole IPv4.
Type de prise	Type de socket pour indiquer la sémantique de communication. Par exemple : SOCK_RAW.
Numéro de protocole	Le numéro de protocole de couche 4, par exemple 17 pour UDP et 6 pour TCP.
IP du point de terminaison local	Adresse IP locale de la connexion.
Port du point de terminaison local	Numéro de port de la connexion.

Écoutez les événements

Les événements Listen fournissent une visibilité sur l'état d'écoute des sockets réseau, indiquant si un socket réseau est prêt à accepter les connexions entrantes. Un processus exécuté sur votre ressource surveillée met le socket réseau en état d'écoute. Le tableau suivant inclut les noms de champs et les descriptions des événements d'écoute que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses AF_INET est utilisée pour le protocole IPv4.
Type de prise	Type de socket pour indiquer la sémantique de communication. Par exemple : SOCK_RAW.
Numéro de protocole	Le numéro de protocole de couche 4, par exemple 17 pour UDP et 6 pour TCP.
IP du point de terminaison local	Adresse IP locale de la connexion.
Port du point de terminaison local	Numéro de port de la connexion.

Renommer les événements

Les événements de renommage fournissent des informations sur le changement de nom des fichiers et des répertoires par les processus exécutés sur les ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements de changement de nom que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Filepath	Chemin du fichier renommé.
Cible	Le nouveau chemin du fichier.

Définir les événements d'ID utilisateur (UID)

Les événements Set User ID (UID) fournissent une visibilité sur les modifications apportées à l'ID utilisateur (UID) associé aux processus en cours sur vos ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements UID définis que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Nouvel EUID	Le nouvel ID utilisateur effectif du processus.
Nouvel UID	Le nouvel ID utilisateur du processus.

Événements Chmod

Les événements Chmod fournissent une visibilité sur les modifications des autorisations (mode) des fichiers et des répertoires sur les ressources surveillées. Le tableau suivant inclut les noms de champs et les descriptions des événements chmod que Runtime Monitoring collecte pour détecter les menaces potentielles.

Nom de champ	Description
Filepath	Chemin du fichier qui invoque cet événement.
Mode de fichier	Les autorisations d'accès mises à jour pour le fichier associé.

Agent d'hébergement GuardDuty de référentiels Amazon ECR

Les sections suivantes répertorient les référentiels Amazon Elastic Container Registry (Amazon ECR) hébergeant l'agent GuardDuty de sécurité déployé sur vos ressources Amazon EKS, Amazon ECS et Amazon ECS-Amazon EC2 Bottlerocket.

La condition préalable vous [Conditions préalables à l'accès aux images du conteneur](#) oblige à fournir un rôle d'exécution de tâche doté de certaines autorisations Amazon Elastic Container Registry (Amazon ECR). Pour restreindre davantage ces autorisations, vous pouvez ajouter l'URI du référentiel Amazon ECR qui héberge l' GuardDuty agent pour les ressources Fargate-Amazon ECS.

Table des matières

- [Référentiel ECR pour les versions 1.16.0 à 1.8.1 de l'agent EKS \(eks.build.2\)](#)
- [Référentiel ECR pour l'agent EKS version 1.8.1 \(eks.build.1\)](#)
- [Référentiel ECR pour GuardDuty agent on AWS Fargate \(Amazon ECS uniquement\)](#)
- [Référentiel ECR pour l' GuardDuty agent sur ECS-EC2 Bottlerocket](#)

Référentiel ECR pour les versions 1.16.0 à 1.8.1 de l'agent EKS (eks.build.2)

Lorsque vous activez la configuration GuardDuty automatique pour la surveillance du temps d'exécution pour EKS, cette version de l'agent GuardDuty sera déployée sur vos clusters Amazon EKS. Pour plus d'informations sur l'activation de l'agent automatisé, consultez [Gestion automatique de l'agent de sécurité pour les ressources Amazon EKS](#).

Le tableau suivant indique les URI du référentiel Amazon ECR dans lequel sont hébergées les versions de l'agent de GuardDuty sécurité 1.16.0.eks.build.2, 1.15.0.eks.build.2, 1.11.0.eks.build.2, 1.10.0.eks.build.2, 1.9.0.eks.build.2, et pour 1.8.0.eks.build.2 Amazon EKS.

Région AWS	URI du référentiel Amazon ECR
USA Ouest (Oregon)	602401143452.dkr.ecr.us-west-2.amazonaws.com
	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europe (Paris)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asie-Pacifique (Mumbai)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asie-Pacifique (Hyderabad)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
	618745550137.dkr.ecr.ap-south-2.amazonaws.com

Région AWS	URI du référentiel Amazon ECR
Canada (Centre)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Canada Ouest (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
	—
Moyen-Orient (EAU)	759879836304.dkr.ecr.me-central-1.amazonaws.com
	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europe (Londres)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
	109118265657.dkr.ecr.eu-west-2.amazonaws.com
USA Ouest (Californie du Nord)	602401143452.dkr.ecr.us-west-1.amazonaws.com
	373421517865.dkr.ecr.us-west-1.amazonaws.com
USA Est (Virginie du Nord)	602401143452.dkr.ecr.us-east-1.amazonaws.com
	031903291036.dkr.ecr.us-east-1.amazonaws.com
USA Est (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com

Région AWS	URI du référentiel Amazon ECR
	<code>591382732059.dkr.ecr.us-east-2.amazonaws.com</code>
Europe (Ireland)	<code>602401143452.dkr.ecr.eu-west-1.amazonaws.com</code>
	<code>673884943994.dkr.ecr.eu-west-1.amazonaws.com</code>
South America (São Paulo)	<code>602401143452.dkr.ecr.sa-east-1.amazonaws.com</code>
	<code>941219317354.dkr.ecr.sa-east-1.amazonaws.com</code>
Europe (Stockholm)	<code>602401143452.dkr.ecr.eu-north-1.amazonaws.com</code>
	<code>366771026645.dkr.ecr.eu-north-1.amazonaws.com</code>
Europe (Francfort)	<code>602401143452.dkr.ecr.eu-central-1.amazonaws.com</code>
	<code>409493279830.dkr.ecr.eu-central-1.amazonaws.com</code>
Europe (Zurich)	<code>900612956339.dkr.ecr.eu-central-2.amazonaws.com</code>
	<code>718440343717.dkr.ecr.eu-central-2.amazonaws.com</code>
Asie-Pacifique (Singapour)	<code>602401143452.dkr.ecr.ap-southeast-1.amazonaws.com</code>
	<code>584580519942.dkr.ecr.ap-southeast-1.amazonaws.com</code>

Région AWS	URI du référentiel Amazon ECR
Asie-Pacifique (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asie-Pacifique (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asie-Pacifique (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asie-Pacifique (Séoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asie-Pacifique (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asie-Pacifique (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain)	558608220178.dkr.ecr.me-south-1.amazonaws.com

Région AWS	URI du référentiel Amazon ECR
	<code>541829937850.dkr.ecr.me-sou th-1.amazonaws.com</code>
Europe (Milan)	<code>590381155156.dkr.ecr.eu-sou th-1.amazonaws.com</code>
	<code>528450769569.dkr.ecr.eu-sou th-1.amazonaws.com</code>
Europe (Espagne)	<code>455263428931.dkr.ecr.eu-sou th-2.amazonaws.com</code>
	<code>531047660167.dkr.ecr.eu-sou th-2.amazonaws.com</code>
Afrique (Le Cap)	<code>877085696533.dkr.ecr.af-sou th-1.amazonaws.com</code>
	<code>379032919888.dkr.ecr.af-sou th-1.amazonaws.com</code>
Asie-Pacifique (Melbourne)	<code>491585149902.dkr.ecr.ap-sou theast-4.amazonaws.com</code>
	<code>750462861327.dkr.ecr.ap-sou theast-4.amazonaws.com</code>
Israël (Tel Aviv)	<code>066635153087.dkr.ecr.il-cen tral-1.amazonaws.com</code>
	<code>292660727137.dkr.ecr.il-cen tral-1.amazonaws.com</code>
Asie-Pacifique (Malaisie)	<code>151610086707.dkr.ecr.ap-sou theast-5.amazonaws.com</code>
Asie-Pacifique (Thaïlande)	<code>121268973566.dkr.ecr.ap-sou theast-7.amazonaws.com</code>

Région AWS	URI du référentiel Amazon ECR
Mexique (Centre)	730335286997.dkr.ecr.mx-central-1.amazonaws.com
Asie-Pacifique (Taïpei)	533267051163.dkr.ecr.ap-east-2.amazonaws.com

Référentiel ECR pour l'agent EKS version 1.8.1 (eks.build.1)

Cette section fournit le référentiel Amazon ECR pour l'agent Amazon EKS version 1.8.1 (v1.8.1-eks-build.1). Si vous utilisez la version v1.8.1-eks-build.1, il est GuardDuty recommandé de passer à la version par défaut de l'agent, qui est généralement la dernière version de l'agent. Pour ce faire, identifiez le dernier agent de [Versions d'agent publiées pour les ressources Amazon EKS](#), puis effectuez les étapes décrites dans [Mise à jour manuelle de l'agent de sécurité pour les ressources Amazon EKS](#).

Le tableau suivant indique les URI du référentiel Amazon ECR où est hébergée la version GuardDuty de l'agent de sécurité pour 1.8.1-eks-build.1 Amazon EKS.

Région AWS	URI du référentiel Amazon ECR
USA Ouest (Oregon)	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europe (Paris)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asie-Pacifique (Mumbai)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asie-Pacifique (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canada (Centre)	001188825231.dkr.ecr.ca-central-1.amazonaws.com

Région AWS	URI du référentiel Amazon ECR
Moyen-Orient (EAU)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europe (Londres)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
USA Ouest (Californie du Nord)	373421517865.dkr.ecr.us-west-1.amazonaws.com
USA Est (Virginie du Nord)	031903291036.dkr.ecr.us-east-1.amazonaws.com
USA Est (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europe (Irlande)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
South America (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europe (Stockholm)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europe (Francfort)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europe (Zurich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asie-Pacifique (Singapour)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asie-Pacifique (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asie-Pacifique (Jakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com

Région AWS	URI du référentiel Amazon ECR
Asie-Pacifique (Tokyo)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asie-Pacifique (Séoul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asie-Pacifique (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asie-Pacifique (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europe (Milan)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europe (Espagne)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Afrique (Le Cap)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asie-Pacifique (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israël (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Référentiel ECR pour GuardDuty agent on AWS Fargate (Amazon ECS uniquement)

Comme condition préalable à l'utilisation de Runtime Monitoring pour Amazon ECS-Fargate, vous devez [Conditions préalables à l'accès aux images du conteneur](#). L'image du conteneur annexe de l' GuardDutyagent est stockée dans Amazon ECR, et ses couches d'images sont stockées dans

Amazon S3. Pour plus d'informations, consultez [Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate](#).

Le tableau suivant indique les référentiels Amazon ECR qui hébergent l' GuardDuty agent pour (AWS Fargate Amazon ECS uniquement) pour chacun d'entre eux. Région AWS

Région AWS	URI du référentiel Amazon ECR
USA Ouest (Oregon)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guard-duty-agent-fargate
Europe (Paris)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guard-duty-agent-fargate
Asie-Pacifique (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guard-duty-agent-fargate
Asie-Pacifique (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guard-duty-agent-fargate
Canada (Centre)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Moyen-Orient (EAU)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Europe (Londres)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guard-duty-agent-fargate
USA Ouest (Californie du Nord)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guard-duty-agent-fargate

Région AWS	URI du référentiel Amazon ECR
USA Est (Virginie du Nord)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guard-duty-agent-fargate
USA Est (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guard-duty-agent-fargate
Europe (Irlande)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guard-duty-agent-fargate
South America (São Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guard-duty-agent-fargate
Europe (Stockholm)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guard-duty-agent-fargate
Europe (Francfort)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Europe (Zurich)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guard-duty-agent-fargate
Asie-Pacifique (Singapour)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guard-duty-agent-fargate
Asie-Pacifique (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guard-duty-agent-fargate

Région AWS	URI du référentiel Amazon ECR
Asie-Pacifique (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Séoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Middle East (Bahrain)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europe (Milan)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europe (Espagne)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
Afrique (Le Cap)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate

Région AWS	URI du référentiel Amazon ECR
Asie-Pacifique (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
Israël (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Malaisie)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Thaïlande)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate
Canada-Ouest (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate
Mexique (Centre)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asie-Pacifique (Taïpei)	259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate

Référentiel ECR pour l' GuardDuty agent sur ECS-EC2 Bottlerocket

Sur les instances Bottlerocket ECS-A Amazon Amazon EC2, GuardDuty l'agent de sécurité s'exécute en tant que conteneur hôte. L'image du conteneur de l'agent est hébergée sur Amazon ECR. Pour plus d'informations sur les conditions préalables, notamment la connectivité réseau et les autorisations IAM requises, consultez. [Conditions préalables au support de ECS-EC2 Bottlerocket](#)

Le profil d'instance doit inclure les politiques AmazonEC2ContainerRegistryReadOnly gérées AmazonSSMManagedInstanceCore et.

Le tableau suivant indique les référentiels Amazon ECR qui hébergent l' agent GuardDuty pour les instances Amazon ECS-Amazon EC2 Bottlerocket pour chacun d'entre eux. Région AWS

Région AWS	URI du référentiel Amazon ECR
USA Est (Virginie du Nord)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guard-duty-agent-ecs-ec2
USA Est (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guard-duty-agent-ecs-ec2
USA Ouest (Californie du Nord)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guard-duty-agent-ecs-ec2
USA Ouest (Oregon)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guard-duty-agent-ecs-ec2
Europe (Irlande)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guard-duty-agent-ecs-ec2
Europe (Londres)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guard-duty-agent-ecs-ec2
Europe (Paris)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guard-duty-agent-ecs-ec2
Europe (Francfort)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guard-duty-agent-ecs-ec2

Région AWS	URI du référentiel Amazon ECR
Europe (Zurich)	<code>529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Europe (Stockholm)	<code>591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Europe (Milan)	<code>266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Europe (Espagne)	<code>919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Asie-Pacifique (Tokyo)	<code>533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Asie-Pacifique (Séoul)	<code>914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Asie-Pacifique (Osaka)	<code>273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Asie-Pacifique (Singapour)	<code>174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>
Asie-Pacifique (Sydney)	<code>005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2</code>

Région AWS	URI du référentiel Amazon ECR
Asie-Pacifique (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Canada (Centre)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Canada Ouest (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Amérique du Sud (São Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Middle East (Bahrain)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2

Région AWS	URI du référentiel Amazon ECR
Moyen-Orient (EAU)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Afrique (Le Cap)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Israël (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Malaisie)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Thaïlande)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-ecs-ec2
Mexique (Centre)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asie-Pacifique (Taipei)	259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2

Deux agents de sécurité sur le même hôte sous-jacent

Les instances Amazon EC2 peuvent prendre en charge plusieurs types de charges de travail. Lorsque vous configurez un agent de sécurité automatique sur une instance Amazon EC2, la même instance EC2 peut avoir un autre agent de sécurité via EKS.

Vue d'ensemble

Imaginons un scénario dans lequel vous avez activé la surveillance du temps d'exécution. Vous pouvez désormais activer l'agent automatisé pour Amazon EKS via GuardDuty. Vous avez également activé l'agent automatique pour Amazon EC2. Il peut arriver que le même hôte sous-jacent soit installé avec deux agents de sécurité, l'un pour Amazon EKS et l'autre pour Amazon EC2. Cela peut entraîner l'exécution de deux agents de sécurité sur le même hôte, collectant des événements d'exécution et les envoyant à GuardDuty, et générant potentiellement des résultats dupliqués.

Impact

- Lorsque plusieurs agents de sécurité sont exécutés sur le même hôte, il est possible que votre compte ait besoin de deux fois plus de processeur et de mémoire. Pour plus d'informations sur les limites de processeur et de mémoire pour chaque type de ressource, consultez la section [Conditions préalables](#) relative à cette ressource.
- GuardDuty a conçu la fonctionnalité de surveillance du temps d'exécution de telle sorte que même si deux agents de sécurité collectent des événements d'exécution auprès du même hôte sous-jacent se chevauchent, votre compte ne sera débité que pour un seul flux d'événements d'exécution.

Comment GuardDuty gère plusieurs agents

GuardDuty détecte lorsque deux agents de sécurité sont exécutés sur le même hôte et désigne un seul d'entre eux comme étant l'agent de sécurité qui collecte activement les événements d'exécution. Le second agent consommera un minimum de ressources système afin d'éviter tout impact sur les performances de vos applications.

GuardDuty prend en compte les scénarios suivants :

- Lorsqu'une instance EC2 entre dans le champ d'application des agents de sécurité Amazon EKS et Amazon EC2, l'agent de sécurité EKS est prioritaire. Cela ne s'applique que lorsque vous utilisez l'agent de sécurité v1.1.0 ou supérieur pour Amazon EC2. Les anciennes versions de l'agent continueront à s'exécuter et à collecter les événements d'exécution, car les anciennes versions de l'agent ne sont pas affectées par la hiérarchisation.
- Lorsque Amazon EKS et Amazon EC2 ont tous deux GuardDuty géré des agents de sécurité et que votre instance Amazon EC2 est également gérée par SSM, les deux agents de sécurité sont

installés au niveau de l'hôte. Une fois les agents installés, GuardDuty décide quel agent de sécurité continuera de fonctionner. Lorsque les deux agents de sécurité sont en cours d'exécution, un seul d'entre eux finira par collecter les événements d'exécution.

- Lorsque les agents de sécurité associés à EC2 et à EKS s'exécutent en même temps, GuardDuty cela peut générer des résultats dupliqués uniquement pendant la période de chevauchement.

Cela peut se produire lorsque :

- Les agents de sécurité pour EC2 et EKS sont configurés via GuardDuty (automatiquement), ou
- Votre ressource Amazon EKS dispose d'un agent de sécurité automatisé.
- Lorsque l'agent de sécurité EKS est déjà en cours d'exécution, si vous déployez l'agent de sécurité EC2 manuellement sur le même hôte sous-jacent et que vous répondez à toutes les conditions requises, il est GuardDuty possible que vous n'installiez pas un deuxième agent de sécurité.

Surveillance du temps d'exécution EKS dans GuardDuty

EKS Runtime Monitoring fournit une couverture de détection des menaces liées à l'exécution pour les nœuds et les conteneurs Amazon Elastic Kubernetes Service (Amazon EKS) au sein de votre environnement. AWS EKS Runtime Monitoring utilise un agent de GuardDuty sécurité qui augmente la visibilité de l'exécution sur les charges de travail EKS individuelles, par exemple l'accès aux fichiers, l'exécution des processus et les connexions réseau. L'agent GuardDuty de sécurité aide à GuardDuty identifier les conteneurs spécifiques de vos clusters EKS qui sont potentiellement compromis. Il peut également détecter les tentatives d'augmentation des privilèges d'un conteneur individuel vers l'hôte EC2 sous-jacent et vers l'environnement au sens large AWS .

Grâce à la disponibilité de Runtime Monitoring, l'expérience de console pour EKS Runtime Monitoring GuardDuty a été consolidée dans la supervision du Runtime Monitoring. GuardDuty ne migrera pas automatiquement vos paramètres de surveillance du temps d'exécution EKS en votre nom. Cela nécessite une action de votre part. Si vous souhaitez continuer à utiliser uniquement EKS Runtime Monitoring, vous pouvez utiliser les API ou vérifier et mettre AWS CLI à jour l'état de configuration existant pour EKS Runtime Monitoring. Il GuardDuty recommande toutefois [Migration de la surveillance d'exécution EKS vers la surveillance d'exécution](#) d'utiliser Runtime Monitoring pour surveiller vos clusters Amazon EKS.

Rubriques

- [Configuration de la surveillance du temps d'exécution EKS pour les environnements à comptes multiples \(API\)](#)

- [Configuration de la surveillance du temps d'exécution EKS pour un compte autonome \(API\)](#)
- [Migration de la surveillance d'exécution EKS vers la surveillance d'exécution](#)

Configuration de la surveillance du temps d'exécution EKS pour les environnements à comptes multiples (API)

Dans les environnements à comptes multiples, seul le compte GuardDuty administrateur délégué peut activer ou désactiver EKS Runtime Monitoring pour les comptes membres et gérer la gestion des GuardDuty agents pour les clusters EKS appartenant aux comptes membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter [Managing multiple accounts](#).

Configuration de la surveillance du temps d'exécution EKS pour le compte GuardDuty administrateur délégué

Cette section décrit les étapes à suivre pour configurer EKS Runtime Monitoring et gérer l'agent de GuardDuty sécurité pour les clusters EKS appartenant au compte d' GuardDuty administrateur délégué.

Sur la base des approches [Déploiement de l'agent de sécurité sur Amazon EKS](#) décrites dans, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les clusters EKS)	<p>Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS de votre compte.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité

Étapes

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT :

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'
```

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est GuardDutyManaged -false. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDuty Managed . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>3.</p> <div data-bbox="716 260 1511 667"> <p> Note</p> <p>Ajoutez toujours la balise d'exclusion à votre cluster EKS avant de définir le paramètre <code>STATUS of EKS_RUNTIME_MONITORING</code> sur <code>ENABLED</code> ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> </div> <p>Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS qui n'ont pas été exclus de la surveillance.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p>L'exemple suivant active <code>EKS_RUNTIME_MONITORING</code> et <code>EKS_ADDON_MANAGEMENT</code> :</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez inclure dans la surveillance. La paire clé-valeur est GuardDutyManaged -true. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDuty Managed . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>DISABLED</code>.</p> <p>GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS marqués avec la <code>true</code> paire <code>GuardDutyManaged</code> -.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p>L'exemple suivant active <code>EKS_RUNTIME_MONITORING</code> et désactive <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	<ol style="list-style-type: none"> <p>Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet features en tant que EKS_RUNTIME_MONITORING et l'état de l'objet en tant que ENABLED.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre> <p>Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.</p>

Auto-enable Surveillance du temps d'exécution EKS pour tous les comptes membres

Cette section décrit les étapes permettant d'activer EKS Runtime Monitoring et de gérer l'agent de sécurité pour tous les comptes membres. Cela inclut le compte d' GuardDuty administrateur délégué, les comptes de membres existants et les nouveaux comptes qui rejoignent l'organisation.

Sur la base des approches [Déploiement de l'agent de sécurité sur Amazon EKS](#) décrites dans, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les clusters EKS)	<p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectorsAPI en utilisant la vôtre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que ENABLED.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS de votre compte.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité

Étapes

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<ol style="list-style-type: none"> <p>Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est GuardDuty Managed -false. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS.</p> <p>Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :</p> <ul style="list-style-type: none"> Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <div data-bbox="586 1522 1507 1885"> <p> Note</p> <p>Ajoutez toujours la balise d'exclusion à votre cluster EKS avant de définir le paramètre STATUS of EKS_RUNTIME_MONITORING sur ENABLED ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> </div>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS qui n'ont pas été exclus de la surveillance.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active <code>EKS_RUNTIME_MONITORING</code> et <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div data-bbox="586 1587 1507 1803"> <p> Note</p> <p>Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p> </div>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	<ol style="list-style-type: none"> <p>Ajoutez une balise au cluster EKS que vous souhaitez inclure dans la surveillance. La paire clé-valeur est GuardDuty Managed -true. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS.</p> <p>Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :</p> <ul style="list-style-type: none"> Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>DISABLED</code>.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité

Étapes

GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS marqués avec la `true` paire `GuardDutyManaged` -.

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	<p>1. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet features en tant que EKS_RUNTIME_MONITORING et l'état de l'objet en tant que ENABLED.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] }]'</pre> <p>2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.</p>

Configuration de la surveillance d'exécution EKS pour tous les comptes membres actifs existants

Cette section décrit les étapes permettant d'activer EKS Runtime Monitoring et de gérer l'agent de GuardDuty sécurité pour les comptes de membres actifs existants dans votre organisation.

Sur la base des approches [Déploiement de l'agent de sécurité sur Amazon EKS](#) décrites dans, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Gérez l'agent de sécurité via GuardDuty (surveillez tous les clusters EKS)</p>	<p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectors API en utilisant la vôtre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que ENABLED.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS de votre compte.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div data-bbox="521 1482 1508 1703"> <p> Note</p> <p>Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p> </div> <p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modifcat</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
---	--------

ion des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<ol style="list-style-type: none"> <p>Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est GuardDuty Managed -false. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS.</p> <p>Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :</p> <ul style="list-style-type: none"> Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <div data-bbox="586 1522 1507 1885"> <p> Note</p> <p>Ajoutez toujours la balise d'exclusion à votre cluster EKS avant de définir le paramètre STATUS of EKS_RUNTIME_MONITORING sur ENABLED ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> </div>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectors API en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que ENABLED.</p> <p>GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS qui n'ont pas été exclus de la surveillance.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div> <p> Note</p> <p>Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p> </div>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	<ol style="list-style-type: none"> <p>Ajoutez une balise au cluster EKS que vous souhaitez inclure dans la surveillance. La paire clé-valeur est GuardDuty Managed -true. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS.</p> <p>Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes :</p> <ul style="list-style-type: none"> Remplacez <i>ec2:CreateTags</i> par <code>eks:TagResource</code> . Remplacez <i>ec2:DeleteTags</i> par <code>eks:UntagResource</code> . Remplacez <i>access-project</i> par <code>GuardDutyManaged</code> . Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectors API en utilisant la vôtre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité

Étapes

GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS marqués avec la `true` paire `GuardDutyManaged` -.

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	<ol style="list-style-type: none"> <p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectors API en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 5555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}]]'</pre> <p>Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.</p>

Auto-enable Surveillance du temps d'exécution EKS pour les nouveaux membres

Le compte d' GuardDuty administrateur délégué peut activer automatiquement EKS Runtime Monitoring et choisir une approche pour gérer l'agent GuardDuty de sécurité pour les nouveaux comptes qui rejoignent votre organisation.

Sur la base des approches [Déploiement de l'agent de sécurité sur Amazon EKS](#) décrites dans, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Gérez l'agent de sécurité via GuardDuty (surveillez tous les clusters EKS)</p>	<p>Pour activer de manière sélective EKS Runtime Monitoring pour vos nouveaux comptes, appelez l'opération d'UpdateOrganizationConfiguration API en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que ENABLED.</p> <p>GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS de votre compte.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active à la fois EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT pour un seul compte. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p> <p><code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est GuardDutyManaged -false. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDuty Managed . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>3.</p> <div data-bbox="714 262 1507 667"> <p> Note</p> <p>Ajoutez toujours la balise d'exclusion à votre cluster EKS avant de définir le paramètre <code>STATUS of EKS_RUNTIME_MONITORING</code> sur <code>ENABLED</code> ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> </div> <p>Pour activer de manière sélective EKS Runtime Monitoring pour vos nouveaux comptes, appelez l'opération d'UpdateOrganizationConfiguration API en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS qui n'ont pas été exclus de la surveillance.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active à la fois <code>EKS_RUNTIME_MONITORING</code> et <code>EKS_ADDON_MANAGEMENT</code> pour un seul compte. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <pre data-bbox="716 474 1507 791">aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> <p>Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)</p>	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez inclure dans la surveillance. La paire clé-valeur est GuardDutyManaged -true. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDutyManaged . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Pour activer de manière sélective EKS Runtime Monitoring pour vos nouveaux comptes, appelez

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>l'opération d'UpdateOrganizationConfiguration API en utilisant la vôtre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p> <p>GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS marqués avec la true paire GuardDutyManaged -.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT pour un seul compte. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p> <p><code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	<p>1. Pour activer de manière sélective EKS Runtime Monitoring pour vos nouveaux comptes, appelez l'opération d'UpdateOrganizationConfiguration API en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT pour un seul compte. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p> <p><code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <div data-bbox="716 1430 1507 1749"> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name": "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> </div> <p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code>. En cas</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p> <p>2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.</p>

Activer la surveillance d'exécution EKS pour les comptes membres actifs individuels

Cette section décrit les étapes de configuration d'EKS Runtime Monitoring et de gestion de l'agent de sécurité pour les comptes de membres actifs individuels.

Sur la base des approches [Déploiement de l'agent de sécurité sur Amazon EKS](#) décrites dans, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les clusters EKS)	<p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectors API en utilisant la vôtre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que ENABLED.</p> <p>GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS de votre compte.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page</p>

Approche préférée pour gérer les agents GuardDuty de sécurité

Étapes

Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'
```

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est <code>GuardDutyManaged -false</code>. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> . • Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> . • Remplacez <code>123456789012</code> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>3.</p> <div data-bbox="714 262 1507 667"> <p> Note</p> <p>Ajoutez toujours la balise d'exclusion à votre cluster EKS avant de définir le paramètre <code>STATUS of EKS_RUNTIME_MONITORING</code> sur <code>ENABLED</code> ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p> </div> <p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectors API en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>.</p> <p>GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS qui n'ont pas été exclus de la surveillance.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p>L'exemple suivant active <code>EKS_RUNTIME_MONITORING</code> et <code>EKS_ADDON_MANAGEMENT</code> :</p> <div data-bbox="714 1749 1507 1879"> <pre>aws guardduty update-member-detectors -- detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --account-ids <i>111122223333</i> --feature</pre> </div>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<div data-bbox="716 254 1507 432"><pre>s ' [{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }] '</pre></div> <div data-bbox="716 470 1507 688"><p> Note</p><p>Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.</p></div> <p data-bbox="716 758 1474 982">Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez inclure dans la surveillance. La paire clé-valeur est GuardDutyManaged -true. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2>DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDuty Managed . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez

Approche préférée pour gérer les agents GuardDuty de sécurité

Étapes

l'opération d'[updateMemberDetectors](#) API en utilisant la votre *detector ID*.

Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.

GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS marqués avec la true paire GuardDutyManaged -.

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT :

```
aws guardduty update-member-detectors --
detector-id 12abc34d567e8fa901bc2d34e56
789f0 --account-ids 111122223333 --feature
s '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
"Status" : "DISABLED"}] ]'
```

Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>Lorsque le code est correctement exécuté, il renvoie une liste vide de <code>UnprocessedAccounts</code> . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	<ol style="list-style-type: none"> <p>Pour activer de manière sélective EKS Runtime Monitoring pour vos comptes membres, exécutez l'opération d'updateMemberDetectorsAPI en utilisant la votre <i>detector ID</i>.</p> <p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 5555555555 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] }]'</pre> <p>Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.</p>

Configuration de la surveillance du temps d'exécution EKS pour un compte autonome (API)

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour plus d'informations, consultez [Configuration de la surveillance du temps d'exécution EKS pour les environnements à comptes multiples \(API\)](#).

Après avoir activé la surveillance du temps d'exécution, veillez à installer l'agent GuardDuty de sécurité par le biais d'une configuration automatique ou d'un déploiement manuel. Dans le cadre de toutes les étapes répertoriées dans la procédure suivante, veillez à installer l'agent de sécurité.

Sur la base des approches [Déploiement de l'agent de sécurité sur Amazon EKS](#) décrites dans, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les clusters EKS)	<ol style="list-style-type: none">Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>. Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS de votre compte.Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.a

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p data-bbox="716 258 1398 342">ws.amazon.com/guardduty/console ou exécutez l'ListDetectors API.</p> <p data-bbox="716 384 1414 468">L'exemple suivant active EKS_RUNTIME_MONITORING et EKS_ADDON_MANAGEMENT :</p> <div data-bbox="716 510 1507 785"><pre data-bbox="735 531 1414 764">aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}]]'</pre></div>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est <code>GuardDutyManaged -false</code>. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <code>ec2:CreateTags</code> par <code>eks:TagResource</code> . • Remplacez <code>ec2:DeleteTags</code> par <code>eks:UntagResource</code> . • Remplacez <code>access-project</code> par <code>GuardDutyManaged</code> . • Remplacez <code>123456789012</code> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p data-bbox="654 258 678 289">3.</p> <div data-bbox="716 258 1507 667"><p data-bbox="748 296 862 327"> Note</p><p data-bbox="797 352 1469 625">Ajoutez toujours la balise d'exclusion à votre cluster EKS avant de définir le paramètre <code>STATUS of EKS_RUNTIME_MONITORING</code> sur <code>ENABLED</code> ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.</p></div> <p data-bbox="716 737 1425 961">Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p data-bbox="716 1010 1485 1087">Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>ENABLED</code>.</p> <p data-bbox="716 1136 1497 1266">GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS qui n'ont pas été exclus de la surveillance.</p> <p data-bbox="716 1314 1507 1633">Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p data-bbox="716 1682 1414 1759">L'exemple suivant active <code>EKS_RUNTIME_MONITORING</code> et <code>EKS_ADDON_MANAGEMENT</code> :</p>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
<p>Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)</p>	<ol style="list-style-type: none"> 1. Ajoutez une balise au cluster EKS que vous souhaitez inclure dans la surveillance. La paire clé-valeur est GuardDutyManaged -true. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : <ul style="list-style-type: none"> • Remplacez <i>ec2:CreateTags</i> par eks:TagResource . • Remplacez <i>ec2:DeleteTags</i> par eks:UntagResource . • Remplacez <i>access-project</i> par GuardDutyManaged . • Remplacez <i>123456789012</i> par l' Compte AWS ID de l'entité de confiance. <p>Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<p>le nom d'objet <code>features</code> en tant que <code>EKS_RUNTIME_MONITORING</code> et l'état de l'objet en tant que <code>ENABLED</code>.</p> <p>Définissez l'état pour <code>EKS_ADDON_MANAGEMENT</code> en tant que <code>DISABLED</code>.</p> <p>GuardDuty gèrera le déploiement et les mises à jour de l'agent de sécurité pour tous les clusters Amazon EKS marqués avec la <code>true</code> paire <code>GuardDutyManaged</code> -.</p> <p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p> <p>L'exemple suivant active <code>EKS_RUNTIME_MONITORING</code> et désactive <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre>

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	<ol style="list-style-type: none"><li data-bbox="651 270 1505 1436"><p>Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet features en tant que EKS_RUNTIME_MONITORING et l'état de l'objet en tant que ENABLED.</p><p>Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED.</p><p>Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. <code>detectorId</code> Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez l'ListDetectorsAPI.</p><p>L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT :</p><pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre><li data-bbox="651 1451 1484 1583"><p>Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.</p>

Migration de la surveillance d'exécution EKS vers la surveillance d'exécution

Avec le lancement de GuardDuty Runtime Monitoring, la couverture de détection des menaces a été étendue aux conteneurs Amazon ECS et aux instances Amazon EC2. L'expérience d'EKS Runtime Monitoring est désormais consolidée dans Runtime Monitoring. Vous pouvez activer la surveillance du temps d'exécution et gérer des agents de GuardDuty sécurité individuels pour chaque type de ressource (instance Amazon EC2, cluster Amazon ECS et cluster Amazon EKS) dont vous souhaitez surveiller le comportement d'exécution.

GuardDuty a consolidé l'expérience de console pour EKS Runtime Monitoring dans Runtime Monitoring. GuardDuty recommande [Vérification de l'état de configuration de la surveillance du temps d'exécution](#) et [Migration de la surveillance d'exécution EKS vers la surveillance d'exécution](#).

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous de [Désactiver la surveillance de l'exécution EKS](#). Ceci est important car si vous choisissez ultérieurement de désactiver la surveillance du temps d'exécution et que vous ne désactivez pas la surveillance du temps d'exécution EKS, vous continuerez de devoir payer des frais d'utilisation pour le suivi du temps d'exécution d'EKS.

Pour migrer d'EKS Runtime Monitoring vers Runtime Monitoring

1. La GuardDuty console prend en charge la surveillance du temps d'exécution EKS dans le cadre de la surveillance du temps d'exécution.

Vous pouvez commencer à utiliser la surveillance du temps d'exécution [Vérification de l'état de configuration de la surveillance du temps d'exécution](#) au niveau de votre organisation et de vos comptes.

Assurez-vous de ne pas désactiver EKS Runtime Monitoring avant d'activer le Runtime Monitoring. Si vous désactivez EKS Runtime Monitoring, la gestion des modules complémentaires Amazon EKS sera également désactivée. Procédez aux étapes suivantes dans l'ordre indiqué.

2. Assurez-vous de respecter tous les [Prérequis pour activer la surveillance d'exécution](#).
3. Activez la surveillance du temps d'exécution en répliquant les mêmes paramètres de configuration de l'organisation pour la surveillance du temps d'exécution que pour la surveillance du temps d'exécution d'EKS. Pour plus d'informations, consultez [Activer la surveillance du temps d'exécution](#).
 - Si vous avez un compte autonome, vous devez activer la surveillance du temps d'exécution.

Si votre agent GuardDuty de sécurité est déjà déployé, les paramètres correspondants sont automatiquement répliqués et vous n'avez pas besoin de les configurer à nouveau.

- Si votre organisation possède des paramètres d'activation automatique, veillez à reproduire les mêmes paramètres d'activation automatique pour la surveillance du temps d'exécution.
 - Si vous avez une organisation dont les paramètres sont configurés individuellement pour les comptes de membres actifs existants, assurez-vous d'activer la surveillance du temps d'exécution et de configurer l'agent de GuardDuty sécurité pour ces membres individuellement.
4. Après avoir vérifié que les paramètres de surveillance du temps d'exécution et GuardDuty de l'agent de sécurité sont corrects, [désactivez EKS Runtime Monitoring](#) à l'aide de l'API ou de la AWS CLI commande.
 5. (Facultatif) Si vous souhaitez nettoyer les ressources associées à l'agent GuardDuty de sécurité, consultez [Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring](#).

Si vous souhaitez continuer à utiliser EKS Runtime Monitoring sans activer le Runtime Monitoring, consultez [Surveillance du temps d'exécution EKS dans GuardDuty](#). En fonction de votre cas d'utilisation, choisissez les étapes à suivre pour configurer EKS Runtime Monitoring pour un compte autonome ou pour plusieurs comptes membres.

Vérification de l'état de configuration de la surveillance du temps d'exécution

Utilisez les API ou AWS CLI commandes suivantes pour vérifier l'état de configuration existant d'EKS Runtime Monitoring.

Pour vérifier l'état de la configuration EKS Runtime Monitoring existante dans votre compte

- Exécutez [GetDetector](#) pour vérifier l'état de configuration de votre propre compte.
- Vous pouvez également exécuter la commande suivante en utilisant AWS CLI :

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

Assurez-vous de remplacer l'identifiant du détecteur de votre région Compte AWS et de la région actuelle. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

Pour vérifier l'état de la configuration EKS Runtime Monitoring existante pour votre organisation (en tant que compte d' GuardDuty administrateur délégué uniquement)

- Exécutez [DescribeOrganizationConfiguration](#) pour vérifier l'état de configuration de votre organisation.

Vous pouvez également exécuter la commande suivante en utilisant AWS CLI :

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Assurez-vous de remplacer l'identifiant du détecteur par celui de votre compte d' GuardDuty administrateur délégué et de la région par votre région actuelle. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

Désactiver EKS Runtime Monitoring après la migration vers Runtime Monitoring

Après avoir vérifié que les paramètres existants de votre compte ou de votre organisation ont été répliqués dans Runtime Monitoring, vous pouvez désactiver EKS Runtime Monitoring.

Pour désactiver la surveillance du temps d'exécution EKS

- Pour désactiver EKS Runtime Monitoring dans votre propre compte

Exécutez l'[UpdateDetector](#) API avec votre propre région *detector-id*.

Vous pouvez également utiliser la AWS CLI commande suivante.

12abc34d567e8fa901bc2d34e56789f0 Remplacez-le par votre propre région *detector-id*.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- Pour désactiver EKS Runtime Monitoring pour les comptes des membres de votre organisation

Exécutez l'[UpdateMemberDetectors](#) API avec la région *detector-id* du compte d' GuardDuty administrateur délégué de l'organisation.

Vous pouvez également utiliser la AWS CLI commande suivante. Remplacez-le

12abc34d567e8fa901bc2d34e56789f0 par le compte régional *detector-id* de l' GuardDuty

administrateur délégué de l'organisation et **111122223333** par l' Compte AWS ID du compte membre pour lequel vous souhaitez désactiver cette fonctionnalité.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "DISABLED"}]'
```

- Pour mettre à jour les paramètres d'activation automatique d'EKS Runtime Monitoring pour votre organisation

Effectuez l'étape suivante uniquement si vous avez configuré les paramètres d'activation automatique d'EKS Runtime Monitoring pour les nouveaux (NEW) ou pour tous les (ALL) comptes membres de l'organisation. Si vous l'avez déjà configuré en tant que NONE, vous pouvez ignorer cette étape.

 Note

Si vous configurez la configuration d'activation automatique d'EKS Runtime Monitoring de manière à NONE ce qu'EKS Runtime Monitoring ne soit activé automatiquement pour aucun compte de membre existant ou lorsqu'un nouveau compte de membre rejoint votre organisation.

Exécutez l'[UpdateOrganizationConfiguration](#) API avec la région **detector-id** du compte d' GuardDuty administrateur délégué de l'organisation.

Vous pouvez également utiliser la AWS CLI commande suivante. Remplacez **12abc34d567e8fa901bc2d34e56789f0** par le compte régional **detector-id** de l' GuardDuty administrateur délégué de l'organisation. Remplacez le **EXISTING_VALUE** par votre configuration actuelle pour une activation automatique GuardDuty.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
--features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

GuardDuty versions publiées de l'agent de sécurité

GuardDuty publie une version mise à jour de l'agent de temps à autre. When GuardDuty gère automatiquement l'agent, GuardDuty est conçu pour mettre à jour l'agent en votre nom. Lorsque vous gérez l'agent manuellement, vous êtes responsable de mettre à jour la version de l'agent pour vos types de ressources : instances Amazon EC2, clusters Amazon ECS et clusters Amazon EKS.

Les sections suivantes fournissent les versions de version des agents de GuardDuty sécurité et les notes de mise à jour associées pour tous les types de ressources pris en charge.

Rubriques

- [GuardDuty versions de l'agent de sécurité pour les instances Amazon EC2](#)
- [GuardDuty versions de l'agent de sécurité pour Amazon ECS-EC2 Bottlerocket](#)
- [GuardDuty versions de l'agent de sécurité pour AWS Fargate \(Amazon ECS uniquement\)](#)
- [GuardDuty versions de l'agent de sécurité pour les ressources Amazon EKS](#)
- [Ressources supplémentaires - prochaines étapes](#)

GuardDuty versions de l'agent de sécurité pour les instances Amazon EC2

Le tableau suivant présente l'historique des versions de l'agent GuardDuty de sécurité pour Amazon EC2.

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.17.1	v1.17.1	Ajout du support pour Kernel 7.2. Au démarrage, l'agent détecte le type de GuardDuty connectivité et tente de se connecter au point de terminaison guardduty-data-v2 via link-local.	9 sept. 2026

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
		Mises à jour générales des fonctionnalités de sécurité.	
v1.16.0	v1.16.0	<p>Ajout du support pour Kernel 6.19, 7.0, 7.1.</p> <p>Ajout du support pour Ubuntu 26.04, Debian 13, RedHat 10.2, CentOS Stream 10, Rocky Linux 10.1, Fedora 43 et Fedora 44. Pour obtenir la liste de toutes les distributions de système d'exploitation vérifiées pour les ressources Amazon EC2, consultez. Valider les exigences architecturales</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	17 juillet 2026

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.15.0	v1.15.0	<p>Nouvelles fonctionnalités des agents pour optimiser la collecte d'événements, permettant un déploiement plus rapide des filtres et une vitesse de détection améliorée.</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	14 mai 2026
v1.9.2	v1.9.2	<p>Ajout du support pour Kernel 6.15, 6.16, 6.17, 6.18.</p> <p>Ajout du support pour Alma Linux 9, Alma Linux 10 et SUSE Linux Enterprise Server 16. Pour obtenir la liste de toutes les distributions de système d'exploitation vérifiées pour les ressources Amazon EC2, consultez Valider les exigences architecturales</p>	24 février 2026

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.9.1	v1.9.1	Optimisation générale des performances et mises à jour des fonctionnalités de sécurité.	10 novembre 2025
v1.9.0	v1.9.0	Optimisation et améliorations générales des performances.	23 octobre 2025
v1.8.0	v1.8.0	Optimisation et améliorations générales des performances.	12 août 2025
v1.7.2	v1.7.1	Support amélioré pour l'installation d'agents locaux pour les distributions Linux basées sur RPM.	23 juillet 2025

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.7.1	1.7.1	<p>Ajout du support pour Fedora 40 et Fedora 41. Pour obtenir la liste de toutes les distributions de système d'exploitation vérifiées pour les ressources Amazon EC2, consultez. Valider les exigences architecturales</p> <p>Optimisation et améliorations générales des performances.</p>	3 juin 2025

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.7.0	v1.7.0	<p>Ajout du support pour les versions 8.9 et 9.3 d'Oracle Linux et pour la version 9.5 de Rocky Linux. Pour obtenir la liste de toutes les distributions de système d'exploitation vérifiées pour les ressources Amazon EC2, consultez. Valider les exigences architecturales</p> <p>Résolution d'identification de conteneur améliorée.</p> <p>Optimisation et améliorations générales des performances.</p>	3 avril 2025
v1.6.0	v1.6.0	<p>Optimisation et améliorations générales des performances.</p>	6 février 2025

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.5.0	v1.5.0	<p>Ajout du support pour CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 et Ubuntu 24.04.</p> <p>Support pour les instances ARM pour .../Metad ataDNSRebind les résultats.</p> <p>Optimisation et améliorations générales des performances.</p>	20 novembre 2024
v1.3.1	v1.3.1	Support pour les résolveurs DNS personnalisés.	12 septembre 2024
v1.3.0	v1.3.0	<p>Optimisation et améliorations générales des performances.</p> <p>Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futur GuardDuty Types de recherche liés à la surveillance du temps.</p>	19 août 2024

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.2.0	v1.2.0	<p>Supporte les distributions du système d'exploitation Ubuntu 20.04, Ubuntu 22.04, Debian 11 et Debian 12.</p> <p>Supporte les noyaux 6.5 et 6.8.</p> <p>Optimisation et améliorations générales des performances.</p>	13 juin 2024

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.1.0	v1.1.0	<p>Prend en charge la configuration GuardDuty automatique des agents dans le cadre de la surveillance du temps d'exécution pour les instances Amazon EC2.</p> <p>Prend en charge les nouveaux signaux de sécurité et les résultats publiés avec l'annonce de la disponibilité générale de Runtime Monitoring pour les instances EC2.</p> <p>Optimisation et améliorations générales des performances.</p>	26 mars 2024
v1.0.2	v1.0.2	Supporte les dernières AMI Amazon ECS.	2 février 2024

Version distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.0.1	v1.0.1	Les versions de l'agent publiées avant la v1.0.2 sont incompatibles avec les AMI Amazon ECS lancées après le 31 janvier 2024. Optimisation et améliorations générales des performances.	23 janvier 2024
v1.0.0	v1.0.0	Version initiale de l'installation RPM. Les versions de l'agent publiées avant la v1.0.2 sont incompatibles avec les AMI Amazon ECS lancées après le 31 janvier 2024.	26 novembre 2023

GuardDuty versions de l'agent de sécurité pour Amazon ECS-EC2 Bottlerocket

Le tableau suivant présente l'historique des versions de l'agent de GuardDuty sécurité pour les instances Amazon ECS-EC2 Bottlerocket. L'agent s'exécute en tant que conteneur hôte sur Bottlerocket et sur les versions ECS-3 v1 . 62 . 1 AMI ECS-2 optimisées et supérieures.

Version du distributeur SSM	Version d'agent	Notes de mise à jour	Date de disponibilité
v1.17.1	v1.17.1	<p>Ajout du support pour Kernel 7.2.</p> <p>Au démarrage, l'agent détecte le type de GuardDuty connectivité et tente de se connecter au point de terminaison guardduty-data-v2 via link-local.</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	9 sept. 2026
v1.16.0	v1.16.0	<p>Version initiale de l'agent de GuardDuty sécurité pour les instances Amazon ECS-EC2 Bottlerocket.</p> <p>Supporte Bottlerocket ECS-2 et ses ECS-3 variantes (x86_64 et aarch64).</p>	17 juillet 2026

GuardDuty versions de l'agent de sécurité pour AWS Fargate (Amazon ECS uniquement)

Le tableau suivant présente l'historique des versions de l'agent GuardDuty de sécurité pour Fargate (Amazon ECS uniquement).

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.17.1	<p>x86_64 (AMD64) :</p> <p>sha256:27b27c489113ae83a272b5c98112e043f66faf8379838bb38e2d815dd6dfbf3a</p> <p>Graviton (ARM64) :</p> <p>sha256:195078e48505cb05b06e61df255fc85a6d7917b28678956c75b11e69855bdf3</p>	<p>Ajout du support pour Kernel 7.2.</p> <p>Au démarrage, l'agent détecte le type de GuardDuty connectivité et tente de se connecter au point de terminaison guardduty-data-v2 via link-local.</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	09 septembre 2026
v1.16.0	<p>x86_64 (AMD64) :</p> <p>sha256:711fa37e2cce0417ba3310d81439d6b11170e446f685146b36916e4e38c1560d</p> <p>Graviton (ARM64) :</p> <p>sha256:6851e00893ee958085adaccddf91</p>	Mises à jour générales des fonctionnalités de sécurité.	17 juillet 2026

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
	bdc009ebd dcd46b4da 6fb1962b1 32d47454		
v1.15.0	<p>x86_64 (AMD64) :</p> <p>sha256:66 446df341b ee1a1e218 aa46b7807 d0d047026 6c8f374c5 dbd97efcd b8356348</p> <p>Graviton (ARM64) :</p> <p>sha256:b0 def2aa8ca b6b2060c7 03f386fdb 29dc41660 54e0509a9 362b21a6e d7f9def7</p>	<p>Nouvelles fonctionnalités des agents pour optimiser la collecte d'événements, permettant un déploiement plus rapide des filtres et une vitesse de détection améliorée.</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	28 mai 2026

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.9.0	<div><div>x86_64 (AMD64) : sha256:fd 9acaa2326 f180f0ed0 c5a25d8ff 0a2d0498a 6e900c34c 68d4e973e a7fb26a8</div><div>Graviton (ARM64) : sha256:0b 04f8c2895 6684e7526 77bfd83db c45afc8a4 3f7791fa4 4667b8078 ba48a295</div></div>	Optimisation générale des performances et améliorations de la sécurité.	28 octobre 2025

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.8.0	<div><div>x86_64 (AMD64) :</div><div>sha256:4425417f39e38b24c1be428bacad1dad53e0645530dcf4422436353bfe358e3a</div><div>Graviton (ARM64) :</div><div>sha256:af069418fd6825846f8f575c49906a67c8a446d12d9ed0d21ab95bd0d05497b</div></div>	Optimisation et améliorations générales des performances.	12 août 2025

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.7.0	<p>x86_64 (AMD64) :</p> <p>sha256:bf9197abdf853607e5fa392b4f97ccdd6ca56dd179be3ce8849e552d96582ac8</p> <p>Graviton (ARM64) :</p> <p>sha256:56c8683c948bcd82c0dbcebf755204365ac7285994693c11717bd45f86e279c2</p>	<p>Résolution d'identification de conteneur améliorée.</p> <p>Optimisation et améliorations générales des performances.</p>	04 avril 2025

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.6.0	<p>x86_64 (AMD64) :</p> <p>sha256:c8 dea71d372 bc47b2f23 6f7a091b9 a9b06bc81 93c1cfe4c 9346eb50f 89258897</p> <p>Graviton (ARM64) :</p> <p>sha256:f4 032a566b9 0537646c2 a987bef42 eca1b4980 78ccc58a8 48603f877 971a8dbe</p>	Optimisation et améliorations générales des performances.	6 février 2025

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.5.0	<div><div>x86_64 (AMD64) : sha256:5e6fdc41f9e6b748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54</div><div>Graviton (ARM64) : sha256:d56801ff6864d6014740103b70b1c38431851358d182613bede20fe21090e734</div></div>	<div>Support pour les tâches ARM relatives aux .../Metad ataDNSRebind résultats.</div> <div>Optimisation et améliorations générales des performances.</div>	14 novembre 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.4.1	<div><div>x86_64 (AMD64) :</div><div>sha256:ef36a11151ec2d3d7db22273bfb954750dee76f0ac7bec37a7ba7e74c3de1c78</div><div>Graviton (ARM64) :</div><div>sha256:a8844544a59d6b4cba98f8e528b513ac2d97432f208e3ad497cc16b331aa9faa</div></div>	<div><div>Durcissement de l'image du conteneur.</div><div>Optimisation et améliorations générales des performances.</div></div>	24 octobre 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.3.1	<p>x86_64 (AMD64) :</p> <p>sha256:a6 e2307d796 e2875907b c4c1c6962 2c906f319 2ddc42ef2 7b99e0a8f 0979f3e0</p> <p>Graviton (ARM64) :</p> <p>sha256:ad 1b6539d80 6edb504f1 7e6bcfb8b 4026c5e82 2300afc31 c0d23c6a0 8f9b99e9</p>	Support pour les résolveurs DNS personnalisés.	11 septembre 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.3.0	<p>x86_64 (AMD64) :</p> <p>sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831</p> <p>Graviton (ARM64) :</p> <p>sha256:ff81a755d46681e409f55a95beeda9ebbcbf5336e1c0b1e6348af7c6518bdbb1</p>	<p>Optimisation et améliorations générales des performances.</p> <p>Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futur GuardDuty GuardDuty Types de recherche liés à la surveillance du temps.</p>	9 août 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.2.0	<p>x86_64 (AMD64) :</p> <p>sha256:1d bad20ac2d c66d52d00 bb28dde42 81fe0d3c5 f261b1649 b247c2369 d9e26b93</p> <p>Graviton (ARM64) :</p> <p>sha256:91 930f8446f 5f95b93b8 ccb187739 92affa401 eb3f42da8 9d68077a5 6bafa6cd</p>	Optimisation et améliorations générales des performances.	31 mai 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.1.0	<p>x86_64 (AMD64) :</p> <p>sha256:83 ce3cf2ef8 5a349ed17 97a8cf30a 008ac5d8c 9f673f283 5823957e9 dcf71657</p> <p>Graviton (ARM64) :</p> <p>sha256:0d 4b61648d7 bdeab8ab8 d94684f80 5498927c7 d437d3182 04dcccfe8 c9383dc7</p>	<p>Prend en charge les nouveaux signaux et découvertes de sécurité.</p> <p>Optimisation et améliorations générales des performances.</p>	01 mai 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.0.1	<p>x86_64 (AMD64) :</p> <p>sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68</p> <p>Graviton (ARM64) :</p> <p>sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7</p>	Optimisation et améliorations générales des performances.	26 janvier 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.0.0	x86_64 (AMD64) : sha256:35 9b8b014e5 076c625da a1056090e 522631587 a7afa3b2e 055edda6b d1141017 Graviton (ARM64) : sha256:b9 438690fa8 a86067180 a11658bec 0f4f838ae 3fbd225d0 4b9306250 648b3984	Version initiale de l'agent de GuardDuty sécurité pour AWS Fargate (Amazon ECS uniquement).	26 novembre 2023

GuardDuty versions de l'agent de sécurité pour les ressources Amazon EKS

GuardDuty publie une version mise à jour de l'agent de temps à autre. Lorsqu'il GuardDuty gère automatiquement l'agent, il est conçu pour gérer les mises à jour de l'agent en votre nom. Lorsque vous gérez l'agent manuellement, vous êtes responsable de mettre à jour la version de l'agent pour vos clusters Amazon EKS.

Avant de mettre à jour l'agent vers une version spécifique, ajoutez le registre d'images GuardDuty pour `allowed-container-registries` dans votre contrôleur d'admission. Pour plus d'informations, consultez [Agent d'hébergement GuardDuty de référentiels Amazon ECR](#).

Le tableau suivant présente l'historique des versions de l' [GuardDuty agent complémentaire Amazon EKS](#).

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.17.1	<p>x86_64 (AMD64) : sha256:8d772f754e9af50a63ab6af74ea24c12a5a3fb8a803c7cb c35ffaca3746c0540</p> <p>Graviton (ARM64) : sha256:e5531367e9ffa539e409e99bbf49e804f01fdd894ee9322858b9bca703cd4016</p>	<p>Ajout du support pour Kernel 6.19, 7.0, 7.1.</p> <p>Au démarrage, l'agent détecte le type de GuardDuty connectivité et tente de se connecter au point de terminaison guardduty-data-v2 via link-local.</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	09 septembre 2026	–
v1.16.0	<p>x86_64 (AMD64) : sha256:8a4ef4b5b5e6fce0a4b5a13922e65179293ee15a8812a2c7678b1c4b31e1f305</p>	<p>Ajout du support pour Kernel 6.19, 7.0, 7.1.</p> <p>Mises à jour générales des fonctionnalités de sécurité.</p>	17 juillet 2026	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
	Graviton (ARM64) : sha256:0a73c1d905a39db94f6ea37d98784dac84961e9199935fae20345de7aa3a57b7			
v1.15.0	x86_64 (AMD64) : sha256:512642a5f9d9a316aa9100368acfdbae2481be7a5cfe9929571c1bb6e19c66fe Graviton (ARM64) : sha256:f017e755615ae999fe5f163886f681508e8f53f6ea7e64e7ada733cdedb368d8	Nouvelles fonctionnalités des agents pour optimiser la collecte d'événements, permettant un déploiement plus rapide des filtres et une vitesse de détection améliorée. Mises à jour générales des fonctionnalités de sécurité.	14 mai 2026	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.12.2	<p>x86_64 (AMD64) : sha256:06c25ab9fff7ee93048e5f34148c96273663235937199b4bd2e28b5ee2e5c080</p> <p>Graviton (ARM64) : sha256:f89962d971350ff6ab408cf6ec7bca9dd06152f0172b7f9c68ae770cc0fc4598</p>	Mises à jour générales des fonctionnalités de sécurité.	26 mars 2026	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.12.1	x86_64 (AMD64) : sha256:f29a597745e5acff48809bebac7d8091bbc38229453dd26710c549b817362491 Graviton (ARM64) : sha256:089cebdc7e891177e107a099c9a4e362d9d74b5362cd374b448a16078040f6c6	Optimisation générale des performances et mises à jour des fonctionnalités de sécurité.	17 novembre 2025	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.11.0	<p>x86_64 (AMD64) : sha256:7c398fd50de e5fe493c361aa7fe19 1e094ddfa000c65b44 9a9ed6a5cd53610e7</p> <p>Graviton (ARM64) : sha256:98a547b47d4 770f45e75eb9730c80 7d9265722ca2f391e0 aa5cb19e487ab455f</p>	<p>Ajout du support pour les distributions de systèmes d'exploitation Fedora 40 et Fedora 41. Pour plus d'informations, voir Validation des exigences architecturales (pour EKS).</p> <p>Optimisation générale des performances et améliorations de la sécurité.</p>	29 août 2025	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.10.0	x86_64 (AMD64) : sha256:6d cbe5b055e 1ef0af903 071ede0b0 8f755ad5b 7e9774a67 df5399efd aa1f3d7d Graviton (ARM64) : sha256:f0 536882268 9610a4bab 543abf93d 3e070b1b5 59e62a2e6 7d82dfa98 37600f72	Résolution d'identification de conteneur améliorée. Optimisation et améliorations générales des performances.	04 avril 2025	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.9.0	<p>x86_64 (AMD64) : sha256:51c5789ef6570f9bec879ac48a8f4769718cbc31e45430032569917e219af63f</p> <p>Graviton (ARM64) : sha256:9c2f74e7ea0827b7e422ae4c91fffc6c2bc41a1cdb96c7191d05259d337154e1</p>	Optimisation et améliorations générales des performances.	2 mars 2025	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.8.1	x86_64 (AMD64) : sha256:f2ce8cf89db e17e3388c ecb350535 44dadf21a f7770545f 8d4b50384 076aff47 Graviton (ARM64) : sha256:30f586e4b69 4e704bcaf adfa9081a b0aef3cf bcde39743 a0f1e24f7 7d79627f	Ajout du support pour CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 et Ubuntu 24.04. Support pour les instances ARM pour la .../Metad ataDNSReb ind recherche. Optimisation et améliorations générales des performances.	23 novembre 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.7.1	<p>x86_64 (AMD64) :</p> <p>sha256:b8b86b5d0872c8b67fecf64ec3d172666360545435a1752447d510951a7fd749</p> <p>Graviton (ARM64) :</p> <p>sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9</p>	<p>Optimisation et améliorations générales des performances.</p> <p>Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futur GuardDuty Types de recherche liés à la surveillance du temps.</p> <p>Support pour les résolveurs DNS personnalisés.</p>	13 septembre 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.7.0	x86_64 (AMD64) : sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec Graviton (ARM64) : sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a	Optimisation et améliorations générales des performances. Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futur GuardDuty Types de recherche liés à la surveillance du temps .	17 août 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.6.1	<p>x86_64 (AMD64) : sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bd b07c3ab1</p> <p>Graviton (ARM64) : sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019</p>	Optimisation et améliorations générales des performances.	14 mai 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.6.0	<p>x86_64 (AMD64) : sha256:7d abcbec30d 8b0536767 52fbc19e8 9f77272d9 a6a53cc93 731f58721 80ef9010</p> <p>Graviton (ARM64) : sha256:97 10f53afcc df4f22b26 5a1a6fc27 f1469403a f1f7d5d08 c4869a726 9cdd2650</p>	<ul style="list-style-type: none"> • Prend en charge la configuration GuardDuty automatique des agents pour les EKS/EC2 ressources. • Soutient les nouveaux signaux et résultats de sécurité. Pour plus d'informations, consultez Types d'événements d'exécution collectés qui GuardDuty utilisent et GuardDuty Types de recherche liés à la surveillance du temps. • Optimisation et améliorations générales des performances. 	29 avril 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.5.0	<p>x86_64 (AMD64) : sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d</p> <p>Graviton (ARM64) : sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6</p>	<ul style="list-style-type: none"> Optimisation et améliorations générales des performances. Améliorations de sécurité, y compris les nouveaux types d'événements ci-dessous Types d'événement d'exécution collectés. Améliorations des performances liées à l'utilisation du processeur. 	07 mars 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.4.1	<p>x86_64 (AMD64) : sha256:66 d49192776 3742660fa a87cc2c39 bb97b7873 039157ae8 b90bc999c b73d0b9c</p> <p>Graviton (ARM64) : sha256:53 7a330b2dd 82357024f b6daeb876 1034b7def d43b10dff e0792c9e6 d0778b40</p>	Optimisation et améliorations générales des performances.	16 janvier 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.4.0	<p>x86_64 (AMD64) : sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f</p> <p>Graviton (ARM64) : sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e</p>	<p>Les points de montage du manifeste permettent une meilleure collecte de données</p> <p>AppArmor configuration dans le manifeste</p> <p>Collecter un argument de ligne de commande</p> <p>Optimisation et améliorations générales des performances</p>	21 décembre 2023	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.3.1	<p>x86_64 (AMD64) : sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490aba01ac75992b3ea29</p> <p>Graviton (ARM64) : sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd</p>	Correctifs et mises à jour de sécurité importants.	23 octobre 2023	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.3.0	<p>x86_64 (AMD64) :</p> <p>sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694</p> <p>Graviton (ARM64) :</p> <p>sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb</p>	<p>Compatible avec la plateforme Ubuntu</p> <p>Compatible avec Kubernetes version 1.28</p> <p>Améliorations des performances générales et amélioration de la stabilité.</p>	05 octobre 2023	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.2.0	x86_64 (AMD64) : sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3 Graviton (ARM64) : sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa	Outre les AMD64-based instances, la version v1.2.0 prend désormais également en charge les ARM64-based instances. Prise en charge ajoutée et vérifiée pour Bottlerocket Compatible avec Kubernetes version 1.27 Améliorations des performances générales et améliorations de la stabilité.	16 juin 2023	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard ¹
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	En plus de Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty , cette version de l'agent prend également en charge Kubernetes version 1.26. Améliorations des performances générales et améliorations de la stabilité.	2 mai 2023	14 mai 2024
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Publication initiale de l'agent de module complémentaire Amazon EKS.	30 mars 2023	14 mai 2024

¹ Pour plus d'informations sur la mise à jour de la version actuelle de votre agent qui approche de la fin du support standard, consultez [Mise à jour manuelle de l'agent de sécurité pour les ressources Amazon EKS](#).

Ressources supplémentaires - prochaines étapes

Pour plus d'informations sur les prochaines étapes, consultez les rubriques suivantes :

- [Prérequis pour activer la surveillance d'exécution](#)- Avec les nouvelles versions de l'agent, il est possible que la section des prérequis soit mise à jour. Vérifiez et validez que vos ressources répondent aux dernières exigences.
- [Gestion des agents GuardDuty de sécurité](#)- Lorsque vous gérez l'agent manuellement, vous êtes responsable de la gestion des mises à jour de la version de l'agent exécutée sur vos ressources. En fonction de votre type de ressource (Amazon EKS ou Amazon EC2-Amazon ECS), effectuez les étapes de mise à jour de l'agent de sécurité. Assurez-vous également de valider la configuration de votre point de [terminaison VPC](#).
- [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#)- Après avoir mis à jour l'agent de sécurité, vous pouvez évaluer la couverture d'exécution de votre ressource. En cas de problème de couverture, suivez les étapes de dépannage associées.

Désactivation, désinstallation et nettoyage des ressources dans Runtime Monitoring

Cette section s'applique Compte AWS si vous choisissez de désactiver la surveillance du temps d'exécution ou uniquement la configuration GuardDuty automatique de l'agent pour un type de ressource.

Désactivation de la configuration GuardDuty automatique des agents

GuardDuty ne supprime pas l'agent de sécurité déployé sur votre ressource. Cependant, GuardDuty cessera de gérer les mises à jour de l'agent de sécurité.

GuardDuty continue de recevoir les événements d'exécution de votre type de ressource. Pour éviter tout impact sur vos statistiques d'utilisation, veillez à supprimer l'agent de GuardDuty sécurité de votre ressource.

Le fait qu'un point de terminaison VPC Compte AWS utilise ou non un point de terminaison VPC partagé GuardDuty ne supprime pas le point de terminaison VPC. Si nécessaire, vous devrez supprimer le point de terminaison du VPC manuellement.

Désactivation de la surveillance de l'exécution et de la surveillance de l'exécution EKS

Cette section s'applique à vous dans les scénarios suivants :

- Vous n'avez jamais activé EKS Runtime Monitoring séparément et vous avez maintenant désactivé le Runtime Monitoring.
- Vous désactivez à la fois la surveillance du temps d'exécution et la surveillance du temps d'exécution EKS. Si vous n'êtes pas sûr de l'état de configuration d'EKS Runtime Monitoring, consultez [Vérification de l'état de configuration de la surveillance du temps d'exécution](#).

 Désactiver la surveillance du temps d'exécution sans désactiver la surveillance du temps d'exécution EKS

Dans ce scénario, à un moment donné, vous avez activé EKS Runtime Monitoring, et plus tard, vous avez également activé le Runtime Monitoring sans désactiver EKS Runtime Monitoring.

Désormais, lorsque vous désactivez la surveillance du temps d'exécution, vous devez également désactiver la surveillance du temps d'exécution d'EKS ; dans le cas contraire, vous continuerez à supporter des coûts d'utilisation pour le suivi du temps d'exécution d'EKS.

Si les scénarios listés précédemment s'appliquent à vous, alors vous GuardDuty effectuerez les actions suivantes sur votre compte :

- GuardDuty supprime le point de terminaison VPC doté de GuardDutyManaged la true balise :. Il s'agit du VPC qui GuardDuty a été créé pour gérer l'agent de sécurité automatisé.
- GuardDuty supprime le groupe de sécurité marqué comme GuardDutyManaged :true.
- Pour un VPC partagé qui a été utilisé par au moins un compte participant, GuardDuty ni le point de terminaison du VPC ni le groupe de sécurité associé à la ressource VPC partagée ne sont supprimés.
- Pour une ressource Amazon EKS, GuardDuty supprime l'agent de sécurité. Cela est indépendant du fait qu'il ait été géré manuellement ou par le biais GuardDuty.

Pour une ressource Amazon ECS, étant donné qu'une tâche ECS est immuable, il est GuardDuty impossible de désinstaller l'agent de sécurité de cette ressource. Cela dépend de la façon dont vous gérez l'agent de sécurité, manuellement ou automatiquement GuardDuty. Une fois que vous avez désactivé la surveillance du GuardDuty temps d'exécution, aucun conteneur annexe n'est attaché lorsqu'une nouvelle tâche ECS commence à s'exécuter. Pour plus d'informations sur l'utilisation des Fargate-ECS tâches, consultez [Déploiement de l'agent de sécurité sur Amazon ECS sur Fargate](#).

Pour une ressource Amazon EC2, GuardDuty désinstalle l'agent de sécurité de toutes les instances Amazon EC2 gérées par Systems Manager (SSM) uniquement lorsqu'il répond aux conditions suivantes :

- Votre ressource n'est pas étiquetée avec la balise GuardDutyManaged : false exclusion.
- GuardDuty doit être autorisé à accéder aux balises dans les métadonnées de l'instance. Pour cette ressource EC2, l'accès aux balises dans les métadonnées de l'instance est défini sur Autoriser.

Lorsque vous arrêtez de gérer manuellement l'agent de sécurité

Quelle que soit l'approche que vous utilisez pour déployer et gérer l'agent de GuardDuty sécurité, pour arrêter de surveiller les événements d'exécution dans votre ressource, vous devez supprimer l'agent GuardDuty de sécurité. Lorsque vous souhaitez arrêter de surveiller les événements d'exécution à partir d'un type de ressource dans un compte, vous pouvez également supprimer le point de terminaison Amazon VPC.

Désinstallation manuelle de l'agent de sécurité pour les ressources Amazon EC2

Cette section fournit des méthodes pour désinstaller l'agent de GuardDuty sécurité de vos ressources Amazon EC2. Lorsque vous gérez l'agent de sécurité manuellement, vous êtes responsable de le supprimer des ressources. GuardDuty n'effectue aucune action sur les ressources que vous gérez.

Si vous avez créé un point de terminaison Amazon VPC manuellement, après avoir désinstallé l'agent de sécurité sur tous les types de ressources surveillés de votre compte, vous pouvez choisir de supprimer le point de terminaison VPC. Il s'agit d'une étape distincte. Pour plus d'informations, consultez [To delete a VPC endpoint](#).

En fonction de la façon dont vous avez installé l'agent de sécurité dans votre ressource, choisissez l'une des méthodes suivantes pour le désinstaller.

Rubriques

- [Méthode 1 - À l'aide de la commande Exécuter](#)
- [Méthode 2 - En utilisant les gestionnaires de packages Linux](#)

Méthode 1 - À l'aide de la commande Exécuter

Lorsque vous avez installé l'agent de sécurité avec [Méthode 1 - Utilisation AWS Systems Manager](#), effectuez les étapes suivantes pour désinstaller l'agent :

Pour désinstaller l'agent GuardDuty de sécurité

1. Vous pouvez désinstaller l'agent GuardDuty de sécurité en suivant les étapes indiquées dans la section [AWS Systems Manager Exécuter la commande](#) du Guide de l'AWS Systems Manager utilisateur. Utilisez l'action Désinstaller dans les paramètres pour désinstaller l'agent GuardDuty de sécurité.

Dans la section Cibles, assurez-vous que l'impact ne concerne que les instances Amazon EC2 dont vous souhaitez désinstaller l'agent de sécurité.

Utilisez le GuardDuty document et le distributeur suivants :

- Nom du document : AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
- Distributeur : AmazonGuardDuty-RuntimeMonitoringSsmPlugin

2. Après avoir fourni tous les détails, lorsque vous choisissez Exécuter, l'agent de sécurité déployé sur les instances Amazon EC2 ciblées est supprimé.

Pour supprimer la configuration du point de terminaison Amazon VPC, vous devez désactiver à la fois la surveillance du temps d'exécution et la surveillance du temps d'exécution Amazon EKS.

3. Si vous souhaitez également supprimer le point de terminaison VPC associé à cet agent de sécurité, consultez. [To delete a VPC endpoint](#)

Méthode 2 - En utilisant les gestionnaires de packages Linux

Lorsque vous avez installé l'agent de sécurité avec [Méthode 2 - Utilisation des gestionnaires de packages Linux](#), effectuez les étapes suivantes pour désinstaller l'agent :

Pour désinstaller l'agent GuardDuty de sécurité

1. Connectez-vous à votre instance. Pour savoir comment procéder, consultez la section [Se connecter à votre instance Linux à l'aide d'un client SSH](#) dans le guide de l'utilisateur Amazon EC2.

2. Commande de désinstallation

La commande suivante permet de désinstaller l'agent de GuardDuty sécurité de l'instance Amazon EC2 à laquelle vous vous connectez :

- Pour RPM :

```
sudo rpm -e amazon-guardduty-agent
```

- Pour Debian :

```
sudo dpkg --purge amazon-guardduty-agent
```

Après avoir exécuté la commande, vous pouvez également consulter les journaux associés à la commande.

3. Si vous souhaitez également supprimer le point de terminaison VPC associé à cet agent de sécurité, consultez. [To delete a VPC endpoint](#)

Désinstaller les ressources de l'agent de sécurité pour ECS-EC2 Bottlerocket

Procédez comme suit pour désinstaller l'agent de GuardDuty sécurité de vos instances Bottlerocket ECS-EC2 .

Pour désinstaller l'agent GuardDuty de sécurité

1. Pour désinstaller l'agent GuardDuty de sécurité, utilisez la [commande AWS Systems Manager Exécuter](#) (dans le guide de AWS Systems Manager l'utilisateur) et définissez le paramètre d'action sur Désinstaller.

Dans la section Cibles, assurez-vous que l'impact ne concerne que les instances de Bottlerocket dont vous souhaitez désinstaller l'agent de sécurité.

Utilisez le GuardDuty document et le distributeur suivants :

- Nom du document :AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
- Distributeur :AmazonGuardDuty-RuntimeMonitoringSsmPlugin.

2. Une fois que vous avez fourni tous les détails et que vous avez choisi Run, GuardDuty l'agent de sécurité est supprimé des instances Bottlerocket ciblées.
3. Pour supprimer également le point de terminaison VPC associé à cet agent de sécurité, consultez. [To delete a VPC endpoint](#)

Nettoyer les ressources des agents de sécurité

Cette section explique comment nettoyer les AWS ressources associées à l'agent de sécurité. Comme indiqué dans [Désactivation, désinstallation et nettoyage des ressources](#), GuardDuty ne supprimera ni ne supprimera toutes les ressources de l'agent de sécurité. La section suivante fournit des instructions sur la manière de supprimer les ressources de l'agent de sécurité.

Pour supprimer un point de terminaison Amazon VPC

Lorsque vous gérez l'agent de sécurité manuellement, vous avez peut-être créé un point de terminaison Amazon VPC manuellement. Après avoir désinstallé l'agent de sécurité pour toutes les ressources surveillées de votre compte, vous pouvez choisir de supprimer ce point de terminaison VPC.

La liste suivante fournit des scénarios relatifs à l'utilisation d'un VPC partagé par rapport à l'absence de VPC partagé.

- Sans VPC partagé : lorsque vous ne souhaitez plus surveiller une ressource dans un compte, pensez à supprimer le point de terminaison Amazon VPC.
- Avec un VPC partagé : lorsqu'un compte propriétaire de VPC partagé supprime la ressource de VPC partagée qui était toujours utilisée, l'état de couverture de la surveillance du temps d'exécution (et le cas échéant, de la surveillance du temps d'exécution EKS) des ressources de votre compte propriétaire de VPC partagé et du compte participant peut devenir inadéquat. Pour plus d'informations sur l'état de couverture, consultez [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#).

Pour supprimer le point de terminaison VPC, voir [Supprimer un point de terminaison d'interface](#) dans le AWS PrivateLink Guide.

Pour supprimer le groupe de sécurité

- Sans VPC partagé : lorsque vous ne souhaitez plus surveiller un type de ressource dans un compte, pensez à supprimer le groupe de sécurité associé à Amazon VPC.
- Avec un VPC partagé : lorsque le compte propriétaire du VPC partagé supprime le groupe de sécurité, tout compte participant utilisant actuellement le groupe de sécurité associé

au VPC partagé, l'état de couverture de la surveillance du temps d'exécution pour les ressources de votre compte propriétaire de VPC partagé et du compte participant peut devenir inadéquat. Pour plus d'informations, consultez [Examen des statistiques de couverture du temps d'exécution et résolution des problèmes](#).

Pour plus d'informations sur les étapes à suivre, consultez [Supprimer un groupe de sécurité Amazon EC2](#) dans le guide de l'utilisateur Amazon EC2.

Pour supprimer l'agent de GuardDuty sécurité d'un cluster EKS

Pour supprimer l'agent de sécurité de votre cluster EKS que vous ne souhaitez plus surveiller, consultez la section [Suppression d'un module complémentaire Amazon EKS d'un cluster](#) dans le guide de l'utilisateur Amazon EKS.

La suppression de l'agent de module complémentaire EKS ne supprime pas l'espace de noms `amazon-guardduty` du cluster EKS. Pour supprimer l'espace de noms `amazon-guardduty`, veuillez consulter [Suppression d'un espace de noms](#).

Pour supprimer l'espace de **amazon-guardduty** noms (cluster EKS)

La désactivation de la configuration automatique des agents ne supprime pas automatiquement l'espace de noms `amazon-guardduty` de votre cluster EKS. Pour supprimer l'espace de noms `amazon-guardduty`, veuillez consulter [Suppression d'un espace de noms](#).

GuardDuty Protection contre les logiciels malveillants pour EC2

Malware Protection for EC2 vous aide à détecter la présence potentielle de malwares en analysant les [volumes Amazon Elastic Block Store \(Amazon EBS\) attachés aux instances Amazon Elastic Compute Cloud \(Amazon EC2\)](#) et les charges de travail de conteneur exécutées sur Amazon EC2. Malware Protection for EC2 propose des options d'analyse qui vous permettent de décider si vous souhaitez inclure ou exclure des instances Amazon EC2 spécifiques au moment de l'analyse. Il offre également la possibilité de conserver les instantanés des volumes Amazon EBS attachés aux instances Amazon EC2 ou aux charges de travail des conteneurs dans vos comptes. GuardDuty Les instantanés ne sont conservés que lorsqu'un logiciel malveillant est détecté et que les résultats de la protection contre les logiciels malveillants pour EC2 sont générés.

La protection contre les programmes malveillants pour EC2 est conçue de manière à ne pas affecter les performances de vos ressources. Pour plus d'informations sur le fonctionnement de Malware Protection for EC2 au sein de Malware Protection for EC2 GuardDuty, consultez [Comment GuardDuty analyse les volumes EBS pour détecter les malwares](#). Pour plus d'informations sur la disponibilité de Malware Protection for EC2 dans différents pays Régions AWS, consultez [Régions et points de terminaison](#).

Remarques

Malware Protection for EC2 prend en charge les analyses de programmes malveillants sur les instances gérées pour le mode automatique d'Amazon EKS. Pour en savoir plus, consultez la section [Support des instances gérées dans Guardduty](#).

Malware Protection for EC2 ne prend pas en charge les analyses de programmes malveillants pour les AWS Fargate charges de travail exécutées avec Amazon EKS ou Amazon ECS.

Pour plus d'informations sur ces fonctionnalités d'Amazon EKS, consultez [Qu'est-ce qu'Amazon EKS ?](#) dans le guide de l'utilisateur Amazon EKS.

Rubriques

- [Comparaison entre l'analyse des GuardDuty-initiated programmes malveillants et l'analyse des On-demand programmes malveillants](#)
- [Comment GuardDuty analyse les volumes EBS pour détecter les malwares](#)

- [Volumes Amazon EBS pris en charge pour l'analyse des programmes malveillants](#)
- [Configuration de la conservation des instantanés et de la couverture de numérisation EC2](#)
- [GuardDuty-initiated analyse des logiciels malveillants](#)
- [On-demand analyse des logiciels malveillants dans GuardDuty](#)
- [Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour EC2](#)
- [GuardDuty comptes de service par Région AWS](#)
- [Quotas dans la protection contre les programmes malveillants pour EC2](#)

Comparaison entre l'analyse des GuardDuty-initiated programmes malveillants et l'analyse des On-demand programmes malveillants

Malware Protection for EC2 propose deux types d'analyses pour détecter les activités potentiellement malveillantes dans vos instances Amazon EC2 et les charges de travail de vos conteneurs

GuardDuty-initiated : analyse des programmes malveillants et analyse des programmes malveillants On-demand . Le tableau suivant montre la comparaison entre les deux types d'analyse.

Factor	GuardDuty-initiated analyse des logiciels malveillants	On-demand analyse des logiciels malveillants
Comment invoquer l'analyse ?	Une fois que vous avez activé l'analyse des GuardDuty-initiated programmes malveillants, chaque fois GuardDuty qu'un résultat indique la présence potentielle d'un logiciel malveillant dans une instance Amazon EC2 ou une charge de travail de conteneur , lance GuardDuty automatiquement une analyse des programmes malveillants sans agent sur les volumes Amazon EBS attachés à votre	Vous pouvez lancer une analyse des On-demand programmes malveillants en fournissant le nom de ressource Amazon (ARN) de votre instance Amazon EC2. Vous pouvez lancer une analyse des On-demand programmes malveillants même si aucune GuardDuty recherche n'est générée pour votre ressource. Pour plus d'informations, consultez On-

Factor	GuardDuty-initiated analyse des logiciels malveillants	On-demand analyse des logiciels malveillants
	ressource potentiellement affectée. Pour plus d'informations, consultez GuardDuty-initiated analyse des logiciels malveillants .	demand analyse des logiciels malveillants dans GuardDuty .
Configuration requise	<p>Pour utiliser l'analyse des GuardDuty-initiated programmes malveillants, vous devez l'activer pour votre compte. Pour gérer plusieurs comptes à l'aide AWS Organizations d'une méthode basée sur une invitation, consultez Activation de l'analyse des GuardDuty-initiated programmes malveillants dans les environnements à comptes multiples.</p> <p>Pour activer l'analyse des GuardDuty-initiated programmes malveillants dans votre propre compte, consultez Activation de l'analyse des GuardDuty-initiated programmes malveillants pour un compte autonome.</p>	Votre compte doit avoir été GuardDuty activé. Pour utiliser l'analyse des On-demand programmes malveillants, aucune configuration n'est requise au niveau des fonctionnalités.

Factor	GuardDuty-initiated analyse des logiciels malveillants	On-demand analyse des logiciels malveillants
Durée d'attente pour lancer une nouvelle analyse	Chaque fois que l'un d'entre eux est GuardDuty généré Résultats qui invoquent une analyse des GuardDuty-initiated logiciels malveillants , une analyse des logiciels malveillants n'est lancée automatiquement qu'une fois toutes les 24 heures.	Vous pouvez lancer une analyse des On-demand programmes malveillants sur la même ressource à tout moment une heure après le début de l'analyse précédente.
Disponibilité de la période d'essai gratuite de 30 jours ¹	<p>Lorsque vous activez l'analyse des GuardDuty-initiated programmes malveillants pour la première fois sur votre compte, vous pouvez bénéficier d'une période d'essai gratuite de 30 jours.</p> <p>Pour plus d'informations, consultez Essai gratuit de 30 jours d'analyse des GuardDuty-initiated logiciels malveillants.</p>	Il n'y a pas de période d'essai gratuite avec analyse des On-demand logiciels malveillants pour les GuardDuty comptes nouveaux ou existants.

Factor	GuardDuty-initiated analyse des logiciels malveillants	On-demand analyse des logiciels malveillants
Options de numérisation ²	Une fois que vous avez configuré GuardDuty-initiated d l'analyse des programmes malveillants, Malware Protection for EC2 offre la possibilité de scanner ou d'ignorer des ressources Amazon EC2 spécifiques à l'aide de balises. Malware Protection for EC2 ne lancera pas d'analyse automatique sur les ressources que vous choisissez d'exclure de l'analyse. Pour plus d'informations, consultez Options d'analyse avec balises définies par l'utilisateur .	Étant donné que vous fournissez l'ARN de la ressource pour démarrer manuellement une analyse des programmes malveillants à la demande, l'utilisation n' Options d'analyse avec balises définies par l'utilisateur est pas applicable.

¹ Vous devrez payer des frais d'utilisation pour créer des instantanés de volume EBS et les conserver. Pour plus d'informations sur la configuration de votre compte afin de conserver les instantanés, consultez [Conservation des instantanés](#).

² Le scan des GuardDuty-initiated programmes malveillants et le scan des On-demand programmes malveillants prennent en charge l'utilisation d'une balise globale pour exclure les ressources Amazon EC2 des analyses de programmes malveillants. Pour plus d'informations, consultez [Balise GuardDutyExcluded globale](#).

Comment GuardDuty analyse les volumes EBS pour détecter les malwares

Cette section explique comment Malware Protection for EC2, y compris le scan des GuardDuty-initiated programmes malveillants et le scan des On-demand programmes malveillants, analyse

les volumes Amazon EBS associés à vos instances Amazon EC2 et à vos charges de travail de conteneur. Avant de poursuivre, tenez compte des personnalisations suivantes :

- Options d'analyse : Malware Protection for EC2 permet de spécifier des balises afin d'inclure ou d'exclure les instances Amazon EC2 et les volumes Amazon EBS du processus d'analyse. Seule l'analyse des GuardDuty-initiated programmes malveillants prend en charge les options d'analyse avec des balises définies par l'utilisateur. Le scan des GuardDuty-initiated programmes malveillants et le scan des On-demand programmes malveillants prennent tous deux en charge le GuardDutyExcluded tag global. Pour plus d'informations, consultez [Options d'analyse avec balises définies par l'utilisateur](#).
- Conservation des instantanés : Malware Protection for EC2 propose une option permettant de conserver les instantanés de vos volumes Amazon EBS dans votre compte. AWS Par défaut, ce paramètre est désactivé. Vous pouvez opter pour la conservation des instantanés pour les analyses de programmes malveillants GuardDuty lancées ou à la demande. Pour plus d'informations, consultez [Conservation des instantanés](#).

Lorsqu'elle en GuardDuty génère une ou plusieurs [Résultats qui invoquent une analyse des GuardDuty-initiated logiciels malveillants](#), cette activité sera une raison pour GuardDuty lancer une analyse des logiciels malveillants. Si vos options d'analyse n'excluent pas cette instance, l'analyse GuardDuty sera lancée.

Pour lancer une analyse des On-demand programmes malveillants sur les volumes Amazon EBS associés à une instance Amazon EC2, fournissez le nom de ressource Amazon (ARN) de l'instance Amazon EC2.

En réponse au lancement d'une analyse des programmes malveillants à la demande ou d'une analyse automatique des GuardDuty-initiated programmes malveillants, GuardDuty crée des instantanés des volumes EBS pertinents attachés à la ressource potentiellement affectée et les partage avec le [GuardDuty compte de service](#). Lorsque vous GuardDuty créez un instantané de vos volumes EBS, il ajoute une balise par défaut appelée GuardDutyScanId. Cette balise permet GuardDuty d'accéder à l'instantané. Assurez-vous de ne pas supprimer cette étiquette. À partir de ces instantanés, GuardDuty crée une réplique chiffrée du volume EBS dans le compte de service.

Une fois l'analyse terminée, GuardDuty supprime les volumes EBS répliqués chiffrés et les instantanés de vos volumes EBS. Par défaut, le paramètre de conservation des instantanés est désactivé. Toutefois, les instantanés sont conservés si le [verrouillage des instantanés Amazon EBS](#) est activé pour eux, quels que soient les résultats et les paramètres de l'analyse. GuardDuty Impossible de modifier les paramètres de verrouillage des instantanés Amazon EBS.

La liste suivante décrit le comportement de conservation des instantanés, quel que soit le verrouillage des instantanés EBS :

La conservation des instantanés est activée :

- Lorsqu'un logiciel malveillant est détecté, GuardDuty conserve les instantanés dans votre Compte AWS.
- Lorsqu'aucun logiciel malveillant n'est détecté, GuardDuty il ne conserve pas les instantanés à moins qu'ils ne soient verrouillés.

La conservation des instantanés est désactivée (paramètre par défaut) :

- Qu'un logiciel malveillant soit détecté ou non, les instantanés ne sont pas conservés.
- GuardDuty Impossible de supprimer les instantanés Amazon EBS verrouillés.

GuardDuty conservera chaque volume EBS répliqué dans le compte de service pendant 55 heures au maximum. En cas de panne de service ou de défaillance d'un volume EBS répliqué et de son analyse des logiciels malveillants, ce volume EBS GuardDuty sera conservé pendant sept jours au maximum. La période de rétention prolongée des volumes sert à trier et à traiter la panne ou la panne. GuardDuty Malware Protection for EC2 supprimera les volumes EBS répliqués du compte de service une fois la panne ou la panne résolue, ou une fois la période de rétention prolongée expirée.

Pour plus d'informations sur la méthodologie de détection des GuardDuty programmes malveillants et les moteurs d'analyse qu'elle utilise, consultez [GuardDuty moteur d'analyse pour la détection des malwares](#).

Volumes Amazon EBS pris en charge pour l'analyse des programmes malveillants

Dans tous les appareils compatibles Régions AWS GuardDuty avec la fonctionnalité Malware Protection for EC2, vous pouvez scanner les volumes Amazon EBS chiffrés ou non chiffrés. Vous pouvez avoir des volumes Amazon EBS chiffrés avec l'une ou l'autre clé [Clé gérée par AWS](#) ou une [clé gérée par le client](#). À l'heure actuelle, certaines régions dans lesquelles Malware Protection for EC2 est disponible peuvent prendre en charge les deux méthodes de chiffrement de vos volumes Amazon EBS, tandis que d'autres ne prennent en charge que les clés gérées par le client. Pour plus d'informations sur les régions prises en charge, reportez-vous aux sections et [GuardDuty comptes de service par Région AWS](#). Pour plus d'informations sur les régions où la protection contre les programmes malveillants pour EC2 GuardDuty est disponible mais pas disponible, consultez [Region-specific disponibilité des fonctionnalités](#).

La liste suivante décrit la clé qui permet de GuardDuty savoir si vos volumes Amazon EBS sont chiffrés ou non :

- Les volumes Amazon EBS non chiffrés ou chiffrés avec Clé gérée par AWS — GuardDuty utilisent leur propre clé pour chiffrer les répliques des volumes Amazon EBS.

Si votre région ne prend pas en charge l'analyse des volumes Amazon EBS chiffrés par défaut avec le [chiffrement Amazon EBS, vous devez modifier la clé par défaut](#) pour qu'elle soit une clé gérée par le client. Cela facilitera l' GuardDuty accès à ces volumes EBS. En modifiant la clé, même les futurs volumes EBS seront créés avec la clé mise à jour afin de prendre en charge les GuardDuty analyses de logiciels malveillants. Pour savoir comment modifier la clé par défaut, reportez-vous [Modifier la valeur par défaut AWS KMS ID clé d'un volume Amazon EBS](#) à la section suivante.

- Les volumes Amazon EBS chiffrés à l'aide d'une clé gérée par le client GuardDuty utilisent la même clé pour chiffrer le volume EBS répliqué. Pour plus d'informations sur les politiques liées au AWS KMS chiffrement prises en charge, consultez [Service-linked autorisations de rôle pour Malware Protection for EC2](#).

Modifier la valeur par défaut AWS KMS ID clé d'un volume Amazon EBS

Lorsque vous créez un volume Amazon EBS à l'aide du [chiffrement Amazon EBS](#), et que vous ne spécifiez pas d'ID de AWS KMS clé, votre volume Amazon EBS est chiffré avec une [clé de chiffrement par défaut](#). Lorsque vous activez le chiffrement par défaut, Amazon EBS chiffre automatiquement les nouveaux volumes et instantanés à l'aide de votre clé KMS par défaut pour le chiffrement Amazon EBS.

Vous pouvez modifier la clé de chiffrement par défaut et utiliser une clé gérée par le client pour le chiffrement Amazon EBS. Cela facilitera l' GuardDuty accès à ces volumes Amazon EBS. Pour modifier l'ID de clé EBS par défaut, ajoutez l'autorisation nécessaire suivante à votre politique IAM : `ec2:modifyEbsDefaultKmsKeyId`. Tout volume Amazon EBS nouvellement créé que vous choisissiez de chiffrer, mais que vous ne spécifiez pas d'ID de clé KMS associé, utilisera l'ID de clé par défaut. Utilisez l'une des méthodes suivantes pour mettre à jour l'ID de clé par défaut d'EBS :

Pour modifier l'ID de clé KMS par défaut d'un volume Amazon EBS

Effectuez l'une des actions suivantes :

- Utilisation d'une API — Vous pouvez utiliser l'[ModifyEbsDefaultKmsKeyId](#) API. Pour plus d'informations sur la manière dont vous pouvez consulter l'état de chiffrement de votre volume, consultez [Create Amazon EBS volume](#).
- Utilisation de la AWS CLI commande : l'exemple suivant modifie l'ID de clé KMS par défaut qui cryptera les volumes Amazon EBS si vous ne fournissez pas d'ID de clé KMS. Assurez-vous de remplacer la région par l'identifiant Région AWS de votre clé KM.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

La commande ci-dessus générera une sortie similaire à la sortie suivante :

```
{  
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"  
}
```

Pour plus d'informations, veuillez consulter [modify-ebs-default-kms-key-id](#).

Configuration de la conservation des instantanés et de la couverture de numérisation EC2

Cette section explique comment personnaliser les options d'analyse des programmes malveillants pour vos instances Amazon EC2. Ces personnalisations s'appliquent à la fois à l'analyse des On-demand programmes malveillants et à celles initiées par GuardDuty. Vous pouvez effectuer les opérations suivantes :

- Activer la conservation des instantanés : lorsque cette option est activée avant une analyse, GuardDuty l'instantané Amazon EBS GuardDuty détecté comme malveillant est conservé.
- Choisissez les instances Amazon EC2 à scanner : utilisez des balises pour inclure ou exclure des instances Amazon EC2 spécifiques des analyses de programmes malveillants.

Conservation des instantanés

GuardDuty vous offre la possibilité de conserver les instantanés de vos volumes EBS dans votre AWS compte. Par défaut, le paramètre de conservation des instantanés est désactivé. Les instantanés ne seront conservés que si ce paramètre est activé avant le début de l'analyse.

Au début de l'analyse, GuardDuty génère les volumes EBS répliqués en fonction des instantanés de vos volumes EBS. Une fois l'analyse terminée et le paramètre de conservation des instantanés activé dans votre compte, les instantanés de vos volumes EBS ne seront conservés que lorsqu'un logiciel malveillant est détecté et que la [Protection contre les programmes malveillants pour les types de détection EC2](#) est générée. Lorsqu'aucun logiciel malveillant n'est détecté, quels que soient les paramètres de vos instantanés, il supprime GuardDuty automatiquement les instantanés de vos volumes EBS, sauf si le [verrouillage des instantanés Amazon EBS a été activé sur les instantanés créés](#).

Coût d'utilisation des instantanés

Lors de l'analyse des programmes malveillants, lors de la GuardDuty création des instantanés de vos volumes Amazon EBS, un coût d'utilisation est associé à cette étape. Si vous activez le paramètre de conservation des instantanés pour votre compte, lorsqu'un logiciel malveillant est détecté et que les instantanés sont conservés, vous devrez payer des frais d'utilisation. Pour plus d'informations sur le coût des instantanés et leur conservation, consultez la tarification [d'Amazon EBS](#).

En tant que compte d' GuardDuty administrateur délégué, vous êtes le seul à pouvoir effectuer cette mise à jour au nom des comptes des membres de l'organisation. Toutefois, si le compte d'un membre est [géré par la méthode d'invitation](#), il peut effectuer lui-même cette modification. Pour plus d'informations, consultez [Relations entre le compte administrateur et le compte membre](#).

Choisissez votre méthode d'accès préférée pour activer le paramètre de conservation des instantanés.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Malware Protection for EC2.
3. Choisissez Paramètres généraux dans la partie inférieure de la console. Pour conserver les instantanés, activez Conservation des instantanés.

API/CLI

Exécutez [UpdateMalwareScanSettings](#) pour mettre à jour la configuration actuelle pour le paramètre de conservation des instantanés.

Vous pouvez également exécuter la AWS CLI commande suivante pour conserver automatiquement les instantanés lorsque GuardDuty Malware Protection for EC2 génère des résultats.

Assurez-vous de le remplacer par le vôtre *detector-id* en cours de validité `detectorId`.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Si vous souhaitez désactiver la conservation des instantanés, remplacez `RETENTION_WITH_FINDING` par `NO_RETENTION`.

Options d'analyse avec balises définies par l'utilisateur

À l'aide de l'analyse des GuardDuty-initiated programmes malveillants, vous pouvez également spécifier des balises afin d'inclure ou d'exclure les instances Amazon EC2 et les volumes Amazon EBS du processus d'analyse et de détection des menaces. Vous pouvez personnaliser chaque analyse de GuardDuty-initiated programmes malveillants en modifiant les balises dans la liste des balises d'inclusion ou d'exclusion. Chaque liste peut inclure jusqu'à 50 balises.

Si vous n'avez pas encore de balises définies par l'utilisateur associées à vos ressources EC2, consultez la section Marquer [vos ressources Amazon EC2](#) dans le guide de l'utilisateur Amazon EC2.

Note

On-demand l'analyse des programmes malveillants ne prend pas en charge les options d'analyse comportant des balises définies par l'utilisateur. Elle prend en charge [Balise GuardDutyExcluded globale](#).

Pour exclure les instances EC2 de l'analyse des logiciels malveillants

Si vous souhaitez exclure une instance Amazon EC2 ou un volume Amazon EBS pendant le processus de numérisation, vous pouvez définir la `GuardDutyExcluded` balise sur n'importe quelle

instance Amazon EC2 ou volume Amazon EBS, GuardDuty et vous ne le scannez pas. true Pour de plus amples informations sur la balise GuardDutyExcluded, veuillez consulter [Service-linked autorisations de rôle pour Malware Protection for EC2](#). Vous pouvez également ajouter une balise d'instance Amazon EC2 à une liste d'exclusion. Si vous ajoutez plusieurs balises à la liste des balises d'exclusion, toute instance Amazon EC2 contenant au moins une de ces balises sera exclue du processus d'analyse des logiciels malveillants.

En tant que compte d' GuardDuty administrateur délégué, vous êtes le seul à pouvoir effectuer cette mise à jour au nom des comptes des membres de l'organisation. Toutefois, si le compte d'un membre est [géré par la méthode d'invitation](#), il peut effectuer lui-même cette modification. Pour plus d'informations, consultez [Relations entre le compte administrateur et le compte membre](#).

Choisissez votre méthode d'accès préférée pour ajouter une balise associée à une instance Amazon EC2 à une liste d'exclusion.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Malware Protection for EC2.
3. Développez la section des Inclusion/Exclusion tags. Sélectionnez Add Tags (Ajouter des balises).
4. Choisissez Balises d'exclusion, puis Confirmer.
5. Spécifiez la paire **Key** et **Value** de la balise que vous souhaitez exclure. Il est facultatif de fournir la **Value**. Après avoir ajouté toutes les balises, choisissez Enregistrer.

Important

Les clés et valeurs d'étiquette sont sensibles à la casse. Pour plus d'informations, consultez la section [Restrictions relatives aux balises](#) dans le guide de l'utilisateur Amazon EC2.

Si aucune valeur n'est fournie pour une clé et que l'instance EC2 est étiquetée avec la clé spécifiée, cette instance EC2 sera exclue du processus d'analyse des GuardDuty-initiated programmes malveillants, quelle que soit la valeur attribuée à la balise.

API/CLI

Exécuté [UpdateMalwareScanSettings](#) en excluant une instance EC2 ou une charge de travail de conteneur du processus d'analyse.

L' AWS CLI exemple de commande suivant ajoute une nouvelle balise à la liste des balises d'exclusion. Remplacez l'exemple de *detector-id* par votre propre detectorId valide.

MapEquals est une liste de paires Key/Value.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Exclude": {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Important

Les clés et valeurs d'étiquette sont sensibles à la casse. Pour plus d'informations, consultez la section [Restrictions relatives aux balises](#) dans le guide de l'utilisateur Amazon EC2.

Pour inclure des instances EC2 dans l'analyse des logiciels malveillants

Si vous souhaitez analyser une instance EC2, ajoutez sa balise à la liste d'inclusion. Lorsque vous ajoutez une balise à une liste de balises d'inclusion, une instance EC2 qui ne contient aucune des balises ajoutées est ignorée de l'analyse des logiciels malveillants. Si vous ajoutez plusieurs balises à la liste des balises d'inclusion, une instance EC2 contenant au moins une de ces balises est incluse dans l'analyse des logiciels malveillants. Parfois, une instance EC2 peut être ignorée pendant le processus de numérisation pour d'autres raisons. Pour plus d'informations, consultez [Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants](#).

En tant que compte d' GuardDuty administrateur délégué, vous êtes le seul à pouvoir effectuer cette mise à jour au nom des comptes des membres de l'organisation. Toutefois, si le compte d'un

membre est [géré par la méthode d'invitation](#), il peut effectuer lui-même cette modification. Pour plus d'informations, consultez [Relations entre le compte administrateur et le compte membre](#).

Choisissez votre méthode d'accès préférée pour ajouter une balise associée à une instance EC2 à une liste d'inclusion.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Malware Protection for EC2.
3. Développez la section des Inclusion/Exclusion tags. Sélectionnez Add Tags (Ajouter des balises).
4. Sélectionnez Identifications d'inclusion, puis Confirmer.
5. Choisissez Ajouter une nouvelle identification d'inclusion et spécifiez la paire **Key** et **Value** de la balise que vous souhaitez inclure. Il est facultatif de fournir la **Value**.

Après avoir ajouté toutes les balises d'inclusion, choisissez Enregistrer.

Si aucune valeur n'est fournie pour une clé, une instance EC2 est étiquetée avec la clé spécifiée, l'instance EC2 sera incluse dans le processus d'analyse Malware Protection for EC2, quelle que soit la valeur attribuée à la balise.

API/CLI

- Exécutez [UpdateMalwareScanSettings](#) pour inclure une instance EC2 ou une charge de travail de conteneur dans le processus d'analyse.

L' AWS CLI exemple de commande suivant ajoute une nouvelle balise à la liste des balises d'inclusion. Assurez-vous de remplacer l'exemple *detector-id* par votre propre exemple valide detectorId. Remplacez l'exemple *TestValue* par *TestKey* la Value paire Key et de la balise associée à votre ressource EC2.

MapEquals est une liste de paires Key/Value.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Include": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Important

Les clés et valeurs d'étiquette sont sensibles à la casse. Pour plus d'informations, consultez la section [Restrictions relatives aux balises](#) dans le guide de l'utilisateur Amazon EC2.

Note

La détection d'un nouveau tag peut prendre jusqu'à 5 minutes.

À tout moment, vous pouvez choisir Balises d'inclusion ou Balises d'exclusion, mais pas les deux. Si vous souhaitez passer d'une balise à l'autre, choisissez cette balise dans le menu déroulant lorsque vous ajoutez de nouvelles balises, puis confirmez votre sélection. Cette action efface toutes vos balises actuelles.

Balise **GuardDutyExcluded** globale

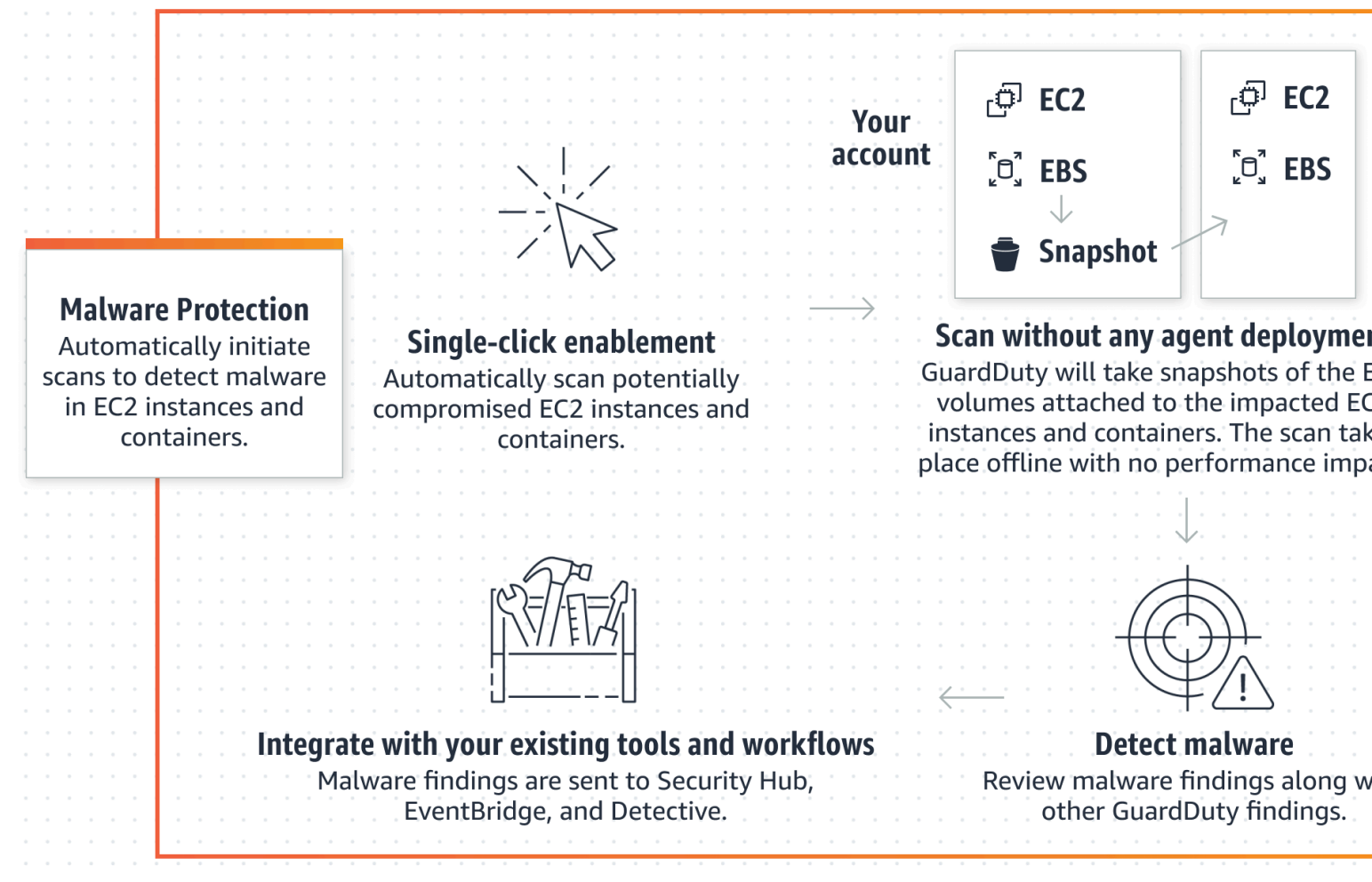
GuardDuty utilise une clé de balise globale `GuardDutyExcluded`, que vous pouvez ajouter à vos ressources Amazon EC2 et définir la valeur de balise sur `true`. Cette ressource Amazon EC2 qui possède cette paire clé-valeur de balise sera exclue de l'analyse des programmes malveillants. Les deux types d'analyse (analyse des GuardDuty-initiated programmes malveillants et analyse des On-demand programmes malveillants) prennent en charge la balise globale. Si vous lancez une analyse des programmes malveillants à la demande sur un Amazon EC2, un ID de scan sera généré. Cependant, le scan sera ignoré `EXCLUDED_BY_SCAN_SETTINGS` pour une raison. Pour plus d'informations, consultez [Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants](#).

GuardDuty-initiated analyse des logiciels malveillants

Lorsque l'analyse des GuardDuty-initiated programmes malveillants est activée, chaque fois qu'elle est GuardDuty générée [Résultats qui invoquent une analyse des GuardDuty-initiated logiciels malveillants](#), une analyse des programmes malveillants sans agent sur les volumes Amazon Elastic Block Store (Amazon EBS) attachés à la ressource Amazon EC2 potentiellement affectée sera lancée. Avant le lancement d'une analyse, vous devez préparer votre compte pour toute personnalisation. Les options d'analyse vous permettent d'ajouter des balises d'inclusion associées aux ressources que vous souhaitez analyser ou des balises d'exclusion associées aux ressources que vous souhaitez ignorer du processus d'analyse. Un lancement automatique du scan tiendra toujours compte de vos options de scan. GuardDuty prend également en charge une paire globale GuardDutyExcluded : true tag clé:valeur. Lorsque vous ajoutez cette balise globale à une ressource Amazon EC2, GuardDuty elle lance le scan puis l'ignore. Vous pouvez également choisir d'activer le paramètre de conservation des instantanés pour conserver les instantanés de vos volumes EBS sur lesquels un logiciel malveillant a été potentiellement détecté. Pour plus d'informations sur les options de numérisation, la balise d'exclusion globale et les paramètres des instantanés, consultez [Configuration de la conservation des instantanés et de la couverture de numérisation EC2](#).

Lorsqu'il GuardDuty génère plusieurs résultats pour la même ressource Amazon EC2, il ne GuardDuty sera en mesure de lancer une analyse que 24 heures après le dernier scan de GuardDuty-initiated malware. Pour plus d'informations sur la manière dont les volumes Amazon EBS attachés à votre instance Amazon EC2 ou à votre charge de travail de conteneur sont analysés, veuillez consulter [Comment GuardDuty analyse les volumes EBS pour détecter les malwares](#).

L'image suivante décrit le fonctionnement de l'analyse des GuardDuty-initiated programmes malveillants.



Pour plus d'informations sur la méthodologie de détection des GuardDuty programmes malveillants et les moteurs d'analyse qu'elle utilise, consultez [GuardDuty moteur d'analyse pour la détection des malwares](#).

Lorsqu'un logiciel malveillant est détecté, GuardDuty génère [Protection contre les programmes malveillants pour les types de détection EC2](#). S'il GuardDuty ne génère aucun résultat indiquant la présence d'un logiciel malveillant sur la même ressource, aucune analyse des GuardDuty-initiated programmes malveillants ne sera invoquée. Vous pouvez également lancer une analyse des On-demand programmes malveillants sur la même ressource. Pour plus d'informations, consultez [On-demand analyse des logiciels malveillants dans GuardDuty](#).

Essai gratuit de 30 jours d'analyse des GuardDuty-initiated logiciels malveillants

Vous pouvez choisir à tout moment d'activer ou de désactiver le scan des GuardDuty-initiated logiciels malveillants pour les Région AWS applications prises en charge. Compte AWS Si vous avez une organisation, chaque compte membre dispose de son propre essai gratuit de 30 jours.

Pour comprendre le fonctionnement de l'essai gratuit de 30 jours, considérez les scénarios suivants :

- Lorsque vous l'activez GuardDuty pour la première fois (nouveau GuardDuty compte), l'analyse des GuardDuty-initiated logiciels malveillants est également activée et est incluse dans l'essai gratuit de 30 jours associé au GuardDuty service.
- Un GuardDuty compte existant peut activer l'analyse des GuardDuty-initiated logiciels malveillants pour la première fois grâce à un essai gratuit de 30 jours. Lorsque vous activez cette fonctionnalité dans une autre région pour la première fois, vous bénéficiez d'un essai gratuit de 30 jours dans cette région.
- Si vous utilisiez Malware Protection for EC2 Région AWS avant que ce plan de protection ne soit divisé en deux types d'analyse : analyse des GuardDuty-initiated programmes malveillants et analyse des On-demand programmes malveillants, vous pouvez continuer à utiliser l'analyse des GuardDuty-initiated programmes malveillants avec le même Région AWS modèle tarifaire. Si vous activez l'analyse des GuardDuty-initiated programmes malveillants pour la première fois dans une nouvelle région, votre compte bénéficiera d'un essai gratuit de 30 jours.

Note

Même si vous bénéficiez d'une période d'essai gratuite de 30 jours, le coût d'utilisation standard pour la création des instantanés de volume Amazon EBS et leur conservation s'appliquent. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Activation de l'analyse des GuardDuty-initiated programmes malveillants dans les environnements à comptes multiples

Dans un environnement à comptes multiples, seul le compte GuardDuty administrateur peut activer l'analyse des GuardDuty-initiated logiciels malveillants pour le compte de ses membres. En outre, un compte administrateur qui gère les comptes des membres avec AWS Organizations assistance peut

choisir d'activer automatiquement l'analyse des GuardDuty-initiated logiciels malveillants sur tous les comptes existants et nouveaux de l'organisation. Pour plus d'informations, consultez [Gérer des GuardDuty comptes avec AWS Organizations](#).

Mise en place d'un accès fiable pour permettre l'analyse des GuardDuty-initiated logiciels malveillants

Si le compte d'administrateur GuardDuty délégué n'est pas le même que le compte de gestion de votre organisation, le compte de gestion doit activer l'analyse des GuardDuty-initiated programmes malveillants pour son organisation. De cette façon, le compte d'administrateur délégué peut créer [Service-linked autorisations de rôle pour Malware Protection for EC2](#) les comptes membres gérés par le biais de AWS Organizations.

Note

Avant de désigner un compte d' GuardDuty administrateur délégué, consultez [Considérations et recommandations](#).

Choisissez votre méthode d'accès préférée pour autoriser le compte GuardDuty administrateur délégué à activer l'analyse des GuardDuty-initiated programmes malveillants pour les comptes des membres de l'organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez le compte de gestion de votre AWS Organizations organisation.

2. a. Si vous n'avez pas désigné de compte d' GuardDuty administrateur délégué, alors :

Sur la page Paramètres, sous Compte d' GuardDuty administrateur délégué, entrez les 12 chiffres **account ID** que vous souhaitez désigner pour administrer la GuardDuty politique de votre organisation. Choisissez Delegate (Déléguer).

- b. i. Si vous avez déjà désigné un compte d' GuardDuty administrateur délégué différent du compte de gestion, alors :

Sur la page Paramètres, sous Administrateur délégué, activez le paramètre Autorisations. Cette action permettra au compte GuardDuty administrateur délégué

d'associer les autorisations pertinentes aux comptes des membres et d'activer l'analyse des GuardDuty-initiated logiciels malveillants dans ces comptes membres.

- ii. Si vous avez déjà désigné un compte d' GuardDuty administrateur délégué identique au compte de gestion, vous pouvez activer directement l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes des membres. Pour plus d'informations, consultez [Auto-enable GuardDuty-initiated analyse des logiciels malveillants pour tous les comptes des membres](#).

 Tip

Si le compte d' GuardDuty administrateur délégué est différent de votre compte de gestion, vous devez fournir des autorisations au compte d' GuardDuty administrateur délégué afin de permettre l'activation de l'analyse des GuardDuty-initiated programmes malveillants pour les comptes des membres.

3. Si vous souhaitez autoriser le compte GuardDuty administrateur délégué à activer l'analyse des GuardDuty-initiated programmes malveillants pour les comptes des membres dans d'autres régions, modifiez votre Région AWS compte et répétez les étapes ci-dessus.

API/CLI

1. À l'aide des informations d'identification de votre compte de gestion, exécutez la commande suivante :

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (Facultatif) Pour activer l'analyse des GuardDuty-initiated programmes malveillants pour le compte de gestion qui n'est pas un compte d'administrateur délégué, le compte de gestion le créera d'abord [Service-linked autorisations de rôle pour Malware Protection for EC2](#) explicitement dans son compte, puis activera l'analyse des GuardDuty-initiated programmes malveillants à partir du compte d'administrateur délégué, comme pour tout autre compte de membre.

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. Vous avez désigné le compte d' GuardDuty administrateur délégué dans le compte actuellement sélectionné Région AWS. Si vous avez désigné un compte en tant que compte d' GuardDuty administrateur délégué dans une région, ce compte doit être votre compte d' GuardDuty administrateur délégué dans toutes les autres régions. Répétez l'étape ci-dessus pour toutes les autres régions.

Configuration de l'analyse des GuardDuty-initiated programmes malveillants pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour activer ou désactiver l'analyse des GuardDuty-initiated programmes malveillants pour un compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Malware Protection for EC2.
3. Sur la page Protection contre les programmes malveillants pour EC2, choisissez Modifier à côté de l'option Analyse des GuardDuty-initiated programmes malveillants.
4. Effectuez l'une des actions suivantes :

Utilisation Activer pour tous les comptes

- Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
- Cliquez sur Enregistrer.

Utilisation Configuration manuelle des comptes

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Cliquez sur Enregistrer.

API/CLI

Exécutez l'opération [updateDetector](#) API en utilisant votre propre identifiant de détecteur régional et en transmettant l'featuresobjet name sous EBS_MALWARE_PROTECTION et en status tant queENABLED.

Vous pouvez activer l'analyse des GuardDuty-initiated programmes malveillants en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser un compte GuardDuty d'administrateur délégué valide *detector ID*.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /  
    --account-ids 5555555555 /  
    --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Auto-enable GuardDuty-initiated analyse des logiciels malveillants pour tous les comptes des membres

Choisissez votre méthode d'accès préférée pour activer la fonction d'analyse des GuardDuty-initiated logiciels malveillants pour tous les comptes des membres. Cela inclut les comptes membres existants et les nouveaux comptes qui rejoignent l'organisation.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

Utilisation de Protection contre les logiciels malveillants pour EC2 page

1. Dans le volet de navigation, choisissez Malware Protection for EC2.
2. Sur la page Protection contre les programmes malveillants pour EC2, choisissez Modifier dans la section d'analyse des GuardDuty-initiated programmes malveillants.

3. Choisissez Activer pour tous les comptes. Cette action active automatiquement l'analyse des GuardDuty-initiated programmes malveillants pour les comptes existants et nouveaux de l'organisation.
4. Cliquez sur Enregistrer.

 Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de Comptes page

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez Auto-enable les préférences avant Ajouter des comptes sur invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes soumis à une analyse des GuardDuty-initiated programmes malveillants.
4. Sur la page Protection contre les programmes malveillants pour EC2, choisissez Modifier dans la section d'analyse des GuardDuty-initiated programmes malveillants.
5. Choisissez Activer pour tous les comptes. Cette action active automatiquement l'analyse des GuardDuty-initiated programmes malveillants pour les comptes existants et nouveaux de l'organisation.
6. Cliquez sur Enregistrer.

 Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de Comptes page

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez Auto-enable les préférences avant Ajouter des comptes sur invitation.

3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes soumis à une analyse des GuardDuty-initiated programmes malveillants.
4. Cliquez sur Enregistrer.

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter [Activer de manière sélective l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes des membres](#).

API/CLI

- Pour activer de manière sélective l'analyse des GuardDuty-initiated logiciels malveillants pour vos comptes membres, appelez l'opération [updateMemberDetectors](#) API en utilisant la votre *detector ID*.
- L'exemple suivant montre comment activer l'analyse des GuardDuty-initiated programmes malveillants pour un seul compte membre. Pour désactiver un compte membre, remplacez ENABLED par DISABLED.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer l'analyse des GuardDuty-initiated logiciels malveillants pour tous les comptes de membres actifs existants

Choisissez votre méthode d'accès préférée pour activer l'analyse des GuardDuty-initiated logiciels malveillants pour tous les comptes de membres actifs existants de l'organisation.

Pour configurer l'analyse des GuardDuty-initiated logiciels malveillants pour tous les comptes de membres actifs existants

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, choisissez Malware Protection for EC2.
3. Sur Malware Protection for EC2, vous pouvez consulter l'état actuel de la configuration de l'analyse des GuardDuty-initiated programmes malveillants. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Cliquez sur Enregistrer.

Auto-enable GuardDuty-initiated analyse des logiciels malveillants pour les nouveaux comptes de membres

Les comptes de membres nouvellement ajoutés doivent être activés GuardDuty avant de sélectionner la configuration de l'analyse des GuardDuty-initiated logiciels malveillants. Les comptes membres gérés par invitation peuvent configurer manuellement le scan des GuardDuty-initiated logiciels malveillants pour leurs comptes. Pour plus d'informations, consultez [Step 3 - Accept an invitation](#).

Choisissez votre méthode d'accès préférée pour activer le scan des GuardDuty-initiated logiciels malveillants pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte GuardDuty administrateur délégué peut activer l'analyse des GuardDuty-initiated programmes malveillants pour les nouveaux comptes membres d'une organisation, à l'aide de la page Protection contre les logiciels malveillants pour EC2 ou des comptes.

Pour activer le scan automatique des GuardDuty-initiated logiciels malveillants pour les nouveaux comptes de membres

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

- À l'aide de la page Protection contre les programmes malveillants pour EC2 :
 1. Dans le volet de navigation, choisissez Malware Protection for EC2.
 2. Sur la page Protection contre les programmes malveillants pour EC2, choisissez Modifier dans le scan des GuardDuty-initiated programmes malveillants.
 3. Choisissez Configurer les comptes manuellement.
 4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, l'analyse des GuardDuty-initiated logiciels malveillants sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
 5. Cliquez sur Enregistrer.
- Utilisation de la page Comptes :
 1. Dans le panneau de navigation, choisissez Accounts (Comptes).
 2. Sur la page Comptes, sélectionnez Auto-enablePréférences.
 3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes dans le cadre de l'analyse des GuardDuty-initiated programmes malveillants.
 4. Cliquez sur Enregistrer.

API/CLI

- Pour activer ou désactiver l'analyse des GuardDuty-initiated programmes malveillants pour les nouveaux comptes membres, appelez l'opération [UpdateOrganizationConfiguration](#) d'API en utilisant la votre *detector ID*.
- L'exemple suivant montre comment activer l'analyse des GuardDuty-initiated programmes malveillants pour un seul compte membre. Pour la désactiver, veuillez consulter [Activer de manière sélective l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes des membres](#). Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes qui rejoignent l'organisation, définissez AutoEnable sur NONE.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name": "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer de manière sélective l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes des membres

Choisissez votre méthode d'accès préférée pour configurer l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes des membres de manière sélective.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sur la page Comptes, consultez la colonne de détection des GuardDuty-initiated logiciels malveillants pour connaître l'état de votre compte de membre.
4. Sélectionnez le compte pour lequel vous souhaitez configurer l'analyse des GuardDuty-initiated programmes malveillants. Vous pouvez sélectionner plusieurs comptes à la fois.
5. Dans le menu Modifier les plans de protection, choisissez l'option appropriée pour l'analyse des GuardDuty-initiated programmes malveillants.

API/CLI

Pour activer ou désactiver de manière sélective l'analyse des GuardDuty-initiated programmes malveillants pour vos comptes membres, appelez l'opération [updateMemberDetectorsAPI](#) en utilisant la votre *detector ID*.

L'exemple suivant montre comment activer l'analyse des GuardDuty-initiated programmes malveillants pour un seul compte membre.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
"Status": "ENABLED"}]'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Pour activer de manière sélective l'analyse des GuardDuty-initiated logiciels malveillants pour vos comptes de membres, exécutez l'opération d'[updateMemberDetectorsAPI](#) en utilisant la votre *detector ID*. L'exemple suivant montre comment activer l'analyse des GuardDuty-initiated programmes malveillants pour un seul compte membre.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activez l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes existants de l'organisation gérés sur invitation

Le rôle lié au service (SLR) GuardDuty Malware Protection for EC2 doit être créé dans les comptes des membres. Le compte administrateur ne peut pas activer la fonctionnalité d'analyse des GuardDuty-initiated programmes malveillants dans les comptes membres qui ne sont pas gérés par AWS Organizations.

À l'heure actuelle, vous pouvez effectuer les étapes suivantes via la GuardDuty console <https://console.aws.amazon.com/guardduty/> pour activer l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes de membres existants.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
Connectez-vous à l'aide des informations d'identification de votre compte administrateur.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sélectionnez le compte membre pour lequel vous souhaitez activer l'analyse des GuardDuty-initiated programmes malveillants. Vous pouvez sélectionner plusieurs comptes à la fois.
4. Choisissez Actions.
5. Choisissez Dissocier le membre.
6. Dans votre compte membre, sélectionnez Protection contre les logiciels malveillants sous Plans de protection dans le volet de navigation.
7. Choisissez Activer l'analyse des GuardDuty-initiated programmes malveillants. GuardDuty créera un reflex pour le compte du membre. Pour plus d'informations sur RLS, veuillez consulter [Service-linked autorisations de rôle pour Malware Protection for EC2](#).
8. Dans le compte de votre compte administrateur, sélectionnez Comptes dans le volet de navigation.
9. Choisissez le compte membre qui doit être ajouté à nouveau à l'organisation.
10. Choisissez Actions, puis Ajouter un membre.

API/CLI

1. Utilisez le compte administrateur pour exécuter [DisassociateMembers](#) l'API sur les comptes membres qui souhaitent activer l'analyse des GuardDuty-initiated logiciels malveillants.

2. Utilisez votre compte de membre pour appeler afin [UpdateDetector](#) d'activer le scan des GuardDuty-initiated logiciels malveillants.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Utilisez le compte administrateur pour exécuter l'[CreateMembers](#) API afin de réintégrer le membre dans l'organisation.

Activation de l'analyse des GuardDuty-initiated programmes malveillants pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour plus d'informations, consultez [Activation de l'analyse des GuardDuty-initiated programmes malveillants dans les environnements à comptes multiples](#).

Une fois que vous avez activé GuardDuty-initiated l'analyse des programmes malveillants, une analyse des programmes malveillants GuardDuty sera lancée sur le volume Amazon EBS attaché à l'instance Amazon EC2 impliquée dans un. GuardDuty Pour obtenir la liste des résultats à l'origine de l'analyse des programmes malveillants, consultez [Résultats qui invoquent une analyse des GuardDuty-initiated logiciels malveillants](#).

Choisissez votre méthode d'accès préférée pour configurer l'analyse des GuardDuty-initiated programmes malveillants pour un compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Malware Protection for EC2.

3. Le volet Protection contre les programmes malveillants pour EC2 indique l'état actuel de l'analyse des GuardDuty-initiated programmes malveillants pour votre compte. Choisissez Activer pour activer l'analyse des GuardDuty-initiated programmes malveillants dans ce compte.
4. Choisissez Enregistrer pour confirmer votre sélection.

API/CLI

Exécutez l'opération [updateDetectorAPI](#) en utilisant votre propre identifiant de détecteur régional et en transmettant l'dataSourceesobjet avec EbsVolumes set to true.

Vous pouvez également activer l'analyse des GuardDuty-initiated logiciels malveillants AWS CLI en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser votre propre code valide *detector ID*.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]
```

Résultats qui invoquent une analyse des GuardDuty-initiated logiciels malveillants

En cas GuardDuty de détection d'un comportement suspect indiquant la présence d'un logiciel malveillant sur une instance Amazon EC2 ou d'une charge de travail de conteneur exécutée sur une instance Amazon EC2 GuardDuty , un résultat est généré. Si ce résultat généré appartient à la liste de GuardDuty résultats suivante, il GuardDuty lancera automatiquement une analyse des programmes malveillants sur les volumes Amazon EBS attachés à l'instance Amazon EC2 impliquée dans le résultat. Après l'analyse, s'il GuardDuty détecte un logiciel malveillant, il en générera également un ou plusieurs [Protection contre les programmes malveillants pour les types de détection EC2](#).

Si l'un des GuardDuty résultats suivants est généré sur votre compte, une analyse des programmes malveillants GuardDuty sera automatiquement lancée dans le volume Amazon EBS de l'instance Amazon EC2 potentiellement compromise.

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/MaliciousFileExecuted.Custom](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#) (Sortant uniquement)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)

- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#) (Sortant uniquement)
- [UnauthorizedAccess:EC2/SSHBruteForce](#) (Sortant uniquement)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [Backdoor:Runtime/C&CActivity.B! DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [CryptoCurrency:Runtime/BitcoinTool.B! DNS](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/BlackholeTraffic! DNS](#)
- [Trojan:Runtime/DropPoint](#)
- [Trojan:Runtime/DropPoint! DNS](#)

- [Trojan:Runtime/DGADomainRequest.C! DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic! DNS](#)
- [Trojan:Runtime/PhishingDomainRequest! DNS](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)

On-demand analyse des logiciels malveillants dans GuardDuty

On-demand l'analyse des programmes malveillants vous permet de détecter la présence de malwares sur les volumes Amazon Elastic Block Store (Amazon EBS) attachés à vos instances Amazon EC2. Aucune configuration n'est nécessaire, vous pouvez lancer une analyse des programmes malveillants à la demande en fournissant le nom de ressource Amazon (ARN) de l'instance Amazon EC2 que vous souhaitez analyser. Vous pouvez lancer une analyse des programmes malveillants à la demande par le biais de la GuardDuty console ou de l'API. Avant d'initier une analyse des logiciels malveillants à la demande, vous pouvez définir votre paramètre [Conservation des instantanés](#) préféré. Les scénarios suivants peuvent vous aider à déterminer dans quels cas utiliser le type d'analyse des On-demand programmes malveillants avec GuardDuty :

- Vous souhaitez détecter la présence de programmes malveillants dans vos instances Amazon EC2 sans activer le scan des GuardDuty-initiated programmes malveillants.
- Vous avez activé l'analyse des GuardDuty-initiated programmes malveillants et une analyse a été lancée automatiquement. Après avoir suivi les mesures correctives recommandées pour le type de détection Malware Protection for EC2 généré, si vous souhaitez lancer une analyse sur la même ressource, vous pouvez lancer une analyse des programmes malveillants à la demande une heure après le début de l'analyse précédente.

On-demand l'analyse des programmes malveillants ne nécessite pas que 24 heures se soient écoulées depuis le début de la précédente analyse des programmes malveillants. Une heure aurait dû s'écouler avant de lancer une analyse des On-demand logiciels malveillants sur la même ressource. Pour éviter de dupliquer une analyse des logiciels malveillants sur la même instance EC2, veuillez consulter [Re-scanning instance Amazon EC2 précédemment scannée](#).

Note

On-demand l'analyse des logiciels malveillants n'est pas incluse dans la période d'essai gratuite de 30 jours avec GuardDuty. Le coût d'utilisation s'applique au volume total d'Amazon EBS analysé pour chaque analyse des logiciels malveillants. Pour plus

d'informations, consultez les [GuardDuty tarifs Amazon](#). Pour plus d'informations sur le coût de création des instantanés des volumes Amazon EBS et leur conservation, veuillez consulter [Tarification d'Amazon EBS](#).

Fonctionnement de l'analyse des On-demand logiciels malveillants

Grâce à l'analyse des On-demand programmes malveillants, vous pouvez lancer une demande d'analyse des programmes malveillants pour votre instance Amazon EC2 même lorsqu'elle est actuellement utilisée. Après avoir lancé une analyse des On-demand programmes malveillants, GuardDuty crée des instantanés des volumes Amazon EBS attachés à l'instance Amazon EC2 dont le nom de ressource Amazon (ARN) a été fourni pour l'analyse. Ensuite, GuardDuty partage ces instantanés avec. [GuardDuty compte de service](#) GuardDuty crée des répliques de volumes EBS chiffrés à partir de ces instantanés du compte de GuardDuty service. Pour plus d'informations sur la manière dont les volumes Amazon EBS sont analysés, veuillez consulter [Comment GuardDuty analyse les volumes EBS pour détecter les malwares](#).

Note

GuardDuty crée les instantanés des données qui ont déjà été écrites sur les volumes Amazon EBS au moment où vous lancez une analyse des programmes malveillants. On-demand

Si un logiciel malveillant est détecté et que vous avez activé le paramètre de conservation des instantanés, les instantanés de votre volume EBS sont automatiquement conservés dans votre. Compte AWS On-demand l'analyse des logiciels malveillants génère le [Protection contre les programmes malveillants pour les types de détection EC2](#). Si aucun logiciel malveillant n'est détecté, quel que soit le paramètre de conservation des instantanés, les instantanés de vos volumes EBS sont supprimés.

GuardDuty utilise une clé de balise globale `GuardDutyExcluded`, que vous pouvez ajouter à vos ressources Amazon EC2 et définir la valeur de balise sur. `true` Cette ressource Amazon EC2 qui possède cette paire clé-valeur de balise sera exclue de l'analyse des programmes malveillants. Les deux types d'analyse (analyse des GuardDuty-initiated programmes malveillants et analyse des On-demand programmes malveillants) prennent en charge la balise globale. Si vous lancez une analyse des programmes malveillants à la demande sur un Amazon EC2, un ID de scan sera généré. Cependant, le scan sera ignoré `EXCLUDED_BY_SCAN_SETTINGS` pour une raison. Pour

plus d'informations, consultez [Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants](#).

Démarrage de l'analyse des On-demand logiciels malveillants dans GuardDuty

Cette section fournit une liste des conditions préalables à remplir avant de lancer une analyse des programmes malveillants à la demande, ainsi que les étapes à suivre pour démarrer l'analyse d'une ressource pour la première fois.

En tant que compte GuardDuty administrateur, vous pouvez lancer une analyse des programmes malveillants à la demande pour le compte de vos comptes de membres actifs dont les conditions préalables suivantes sont définies dans leurs comptes. Les comptes autonomes et les comptes de membres actifs GuardDuty peuvent également lancer une analyse des programmes malveillants à la demande pour leurs propres instances Amazon EC2.

Conditions préalables

Avant de lancer une analyse des On-demand programmes malveillants, votre compte doit remplir les conditions préalables suivantes :

- GuardDuty doit être activé à l' Région AWS endroit où vous souhaitez démarrer l'analyse des programmes malveillants à la demande.
- Assurez-vous que l'[AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) est attaché à l'utilisateur IAM ou au rôle IAM. Vous aurez besoin de la clé d'accès et de la clé secrète associées à l'utilisateur IAM ou au rôle IAM.
- En tant que compte GuardDuty administrateur délégué, vous avez la possibilité de lancer une analyse des programmes malveillants à la demande pour le compte d'un membre actif.
- Avant de lancer une analyse des programmes malveillants à la demande, assurez-vous qu'aucune analyse n'a été lancée sur la même ressource au cours de la dernière heure, sinon elle sera dédoublée. Pour plus d'informations, consultez [Re-scanning instance Amazon EC2 précédemment scannée](#).
- Si votre compte membre n'en dispose pas [Service-linked autorisations de rôle pour Malware Protection for EC2](#), le lancement d'une analyse des programmes malveillants à la demande pour une instance Amazon EC2 appartenant à votre compte créera automatiquement le SLR pour Malware Protection for EC2.

⚠ Important

Assurez-vous que personne ne supprime les [autorisations SLR pour Malware Protection for EC2](#) lorsque l'analyse des programmes malveillants est toujours en cours. Cette analyse des programmes malveillants peut être lancée par GuardDuty ou à la demande. La suppression du réflex empêchera la numérisation de se terminer correctement et de fournir un résultat de numérisation précis.

Lancer l'analyse des On-demand logiciels malveillants

Vous pouvez lancer une analyse des programmes malveillants à la demande dans votre compte via GuardDuty la console ou en utilisant AWS CLI. Vous devrez fournir l'Amazon EC2 Amazon Resource Name (ARN) pour lequel vous souhaitez démarrer le scan. Les étapes détaillées sont fournies dans les AWS CLI instructions relatives à la console et à l'API/ dans la section suivante.

Choisissez votre méthode d'accès préférée pour lancer une analyse des programmes malveillants à la demande.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Lancez le scan à l'aide de l'une des options suivantes :
 - a. À l'aide de la page Protection contre les programmes malveillants pour EC2 :
 - i. Dans le volet de navigation, sous Plans de protection, sélectionnez Malware Protection for EC2.
 - ii. Sur la page Protection contre les programmes malveillants pour EC2, indiquez l'^{ARN} 1 de l'instance Amazon EC2 pour laquelle vous souhaitez démarrer le scan.
 - b. À l'aide de la page Analyses des logiciels malveillants :
 - i. Dans le panneau de navigation, choisissez Analyses des logiciels malveillants.
 - ii. Choisissez Démarrer le scan à la demande et indiquez l'instance Amazon EC2 ARN ¹ pour laquelle vous souhaitez démarrer le scan.
 - iii. S'il s'agit d'une nouvelle analyse, sélectionnez un ID d'instance Amazon EC2 sur la page Analyses des logiciels malveillants.

Développez le menu déroulant Démarrer le scan à la demande et choisissez l'instance Re-scan sélectionnée.

- Une fois que vous avez lancé une analyse avec succès à l'aide de l'une ou l'autre méthode, un ID de numérisation est généré. Vous pouvez utiliser cet ID de numérisation pour suivre la progression de l'analyse. Pour plus d'informations, consultez [Surveillance de l'état et des résultats de l'analyse des logiciels malveillants](#).

API/CLI

Appelez [StartMalwareScan](#) qui accepte resourceArn l'instance Amazon EC2 ¹ pour laquelle vous souhaitez lancer une analyse des programmes malveillants à la demande.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

Une fois que vous avez lancé une analyse avec succès, StartMalwareScan renvoie unscanId. Invoquez le [DescribeMalwareScans](#) suivi de la progression de l'analyse démarrée.

¹Pour plus d'informations sur le format de votre ARN d'instance Amazon EC2, veuillez consulter [Amazon Resource Name \(ARN\)](#). Pour les instances Amazon EC2, vous pouvez utiliser l'exemple de format ARN suivant en remplaçant les valeurs de partition, de région, d'ID Compte AWS et d'ID d'instance Amazon EC2. Pour plus d'informations sur la longueur de votre ID d'instance, veuillez consulter [ID de ressource](#).

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

AWS Organizations politique de contrôle des services — Accès refusé

À l'aide des [politiques de contrôle des services \(SCP\)](#) incluses dans AWS Organizations, le compte GuardDuty administrateur délégué peut restreindre les autorisations et refuser des actions telles que le lancement d'une analyse des programmes malveillants à la demande pour une instance Amazon EC2 détenue par vos comptes.

En tant que compte GuardDuty membre, lorsque vous lancez une analyse des programmes malveillants à la demande pour vos instances Amazon EC2, vous pouvez recevoir un message d'erreur. Vous pouvez vous connecter au compte de gestion pour comprendre pourquoi une SCP

a été configurée pour votre compte membre. Pour de plus amples informations, veuillez consulter [Effets des SCP sur les autorisations](#).

Re-scanning instance Amazon EC2 précédemment scannée

Qu'une analyse soit lancée GuardDuty-initiated ou lancée à la demande, vous pouvez démarrer une nouvelle analyse de programmes malveillants à la demande sur la même instance Amazon EC2 une heure après le début de la précédente analyse de programmes malveillants. Si la nouvelle analyse des programmes malveillants est lancée dans l'heure suivant le lancement de la précédente, votre demande entraînera l'erreur suivante et aucun identifiant de scan ne sera généré pour cette demande.

A scan was started on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.

Les étapes pour réanalyser l'instance restent les mêmes que pour lancer une analyse des programmes malveillants à la demande pour la première fois. Pour plus d'informations sur les étapes, consultez [Lancer l'analyse des On-demand logiciels malveillants](#).

Pour suivre l'état des analyses des logiciels malveillants, veuillez consulter [Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour EC2](#).

Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour EC2

Après le lancement d'une analyse des programmes malveillants sur une instance Amazon EC2, GuardDuty fournit automatiquement les champs d'état et de résultat. Vous pouvez surveiller l'état par le biais de transitions et voir si un logiciel malveillant a été détecté. Le tableau suivant indique les valeurs possibles associées à l'analyse des programmes malveillants.

Valeurs potentielles

Running,Completed ,Skipped, ou Failed

Clean ou Infected

Valeurs potentielles

GuardDuty initiated ou On demand

*Le résultat du scan n'est renseigné que lorsque l'état du scan est atteint. Completed Le résultat de l'analyse Infected signifie que la présence d'un logiciel malveillant a GuardDuty été détectée.

Les résultats d'analyse de chaque analyse des logiciels malveillants ont une période de conservation de 90 jours. Choisissez votre méthode d'accès préférée pour suivre l'état de votre analyse des logiciels malveillants.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez EC2 malware scans.
3. Vous pouvez filtrer les analyses de programmes malveillants à l'aide des propriétés suivantes disponibles dans la barre de recherche du filtre.
 - ID de scan — Identifiant unique associé à l'analyse des programmes malveillants EC2.
 - ID de compte : Compte AWS identifiant à partir duquel l'analyse des logiciels malveillants a été lancée.
 - ARN de l'instance EC2 : Amazon Resource Name (ARN) associé à l'instance Amazon EC2 associée au scan.
 - État de numérisation : état de numérisation du volume EBS, tel que En cours, ignoré et terminé
 - Type de scan : indique s'il s'agit d'un scan de On-demand malware ou d'un scan de GuardDuty-initiated malware.

API/CLI

- Une fois que l'analyse des programmes malveillants a obtenu un résultat d'analyse, utilisez-le [DescribeMalwareScans](#) pour filtrer les analyses de logiciels

malveillants sur la base de EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS, et SCAN_START_TIME.

Les critères de GUARDDUTY_FINDING_ID filtrage sont disponibles lorsque le SCAN_TYPE est GuardDuty lancé.

- Vous pouvez modifier l'exemple *filter-criteria* dans la commande ci-dessous. À l'heure actuelle, vous pouvez filtrer sur la base d'une CriterionKey à la fois. Les options pour CriterionKey sont EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS et SCAN_START_TIME.

Vous pouvez modifier le *max-results* (jusqu'à 50) et le *sort-criteria*. L'AttributeName est obligatoire et doit être scanStartTime.

Dans l'exemple suivant, les valeurs indiquées *red* sont des espaces réservés. Remplacez-les par les valeurs correspondant à votre compte. Par exemple, remplacez l'exemple detector-id *60b8777933648562554d637e0e4bb3b2* par votre propre exemple validedetector-id. Si vous utilisez le même CriterionKey que ci-dessous, assurez-vous de remplacer l'exemple EqualsValue par votre propre exemple valide AWS *scan-id*.

```
aws guardduty describe-malware-scans --detector-id 60b8777933648562554d637e0e4bb3b2 --max-results 1 --sort-criteria '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "SCAN_ID", "FilterCondition": {"EqualsValue": "123456789012"}}] }'
```

- La réponse de cette commande affiche au maximum un résultat avec des informations détaillées sur la ressource affectée et les résultats de logiciels malveillants (si Infected).

GuardDuty comptes de service par Région AWS

Lorsqu'un instantané est créé et partagé avec un compte de GuardDuty service, un nouvel événement est créé dans vos CloudTrail journaux. Cet événement indique le snapshotId et userId (compte GuardDuty de service correspondant Région AWS). Pour plus d'informations, consultez [Comment GuardDuty analyse les volumes EBS pour détecter les malwares](#).

L'exemple suivant est un extrait d'un CloudTrail événement qui montre le corps de la demande : ModifySnapshotAttribute

```
"requestParameters": {
```

```

    "snapshotId": "snap-1234567890abcdef0",
    "createVolumePermission": {
      "add": {
        "items": [
          {
            "userId": "111122223333"
          }
        ]
      }
    },
    "attributeType": "CREATE_VOLUME_PERMISSION"
  }

```

Le tableau suivant indique les comptes GuardDuty de service pour chaque région. `userId` s'agit du compte de GuardDuty service qui dépend de la région sélectionnée.

Région AWS	Code région	GuardDuty ID de compte de service (<code>userId</code>)
USA Est (Virginie du Nord)	us-east-1	652050842985
USA Est (Ohio)	us-east-2	178123968615
USA Ouest (Californie du Nord)	us-west-1	669213148797
USA Ouest (Oregon)	us-west-2	447226417196
Asie-Pacifique (Mumbai)	ap-south-1	913179291432
Asie-Pacifique (Osaka)	ap-northeast-3	089661699081
Asie-Pacifique (Séoul)	ap-northeast-2	039163547507
Asie-Pacifique (Tokyo)	ap-northeast-1	874749492622
Asie-Pacifique (Singapour)	ap-southeast-1	247460962669
Asie-Pacifique (Sydney)	ap-southeast-2	124839743349

Région AWS	Code région	GuardDuty ID de compte de service (userId)
Canada (Centre)	ca-central-1	175877067165
Canada-Ouest (Calgary)	ca-west-1	894794104037
Europe (Francfort)	eu-central-1	002294850712
Europe (Irlande)	eu-west-1	283769539786
Europe (Londres)	eu-west-2	310125036783
Europe (Paris)	eu-west-3	866607715269
Europe (Stockholm)	eu-north-1	693780578038
Chine (Pékin)	cn-north-1	448721096076
Chine (Ningxia)	cn-northwest-1	480864352451
Amérique du Sud (São Paulo)	sa-east-1	546914126324
Asie-Pacifique (Hyderabad) (Opt-in)	ap-south-2	682251015962
Asie-Pacifique (Melbourne) (Opt-in)	ap-southeast-4	353488359550
Asie-Pacifique (Malaisie) Opt-in ()	ap-southeast-5	009160069308
Asie-Pacifique (Thaïlande) Opt-in ()	ap-southeast-7	941377115582
Europe (Espagne) (Opt-in)	eu-south-2	936182149045
Europe (Zurich) (Opt-in)	eu-central-2	867642063380

Région AWS	Code région	GuardDuty ID de compte de service (userId)
Israël (Tel Aviv) (Opt-in)	il-central-1	619233833001
Europe (Milan) (Opt-in)	eu-south-1	977238331021
Asie-Pacifique (Hong Kong) (Opt-in)	ap-east-1	249472122084
Moyen-Orient (Bahreïn) (Opt-in)	me-south-1	404001805210
Afrique (Le Cap) (Opt-in)	af-south-1	957664736811
Asie-Pacifique (Jakarta) (Opt-in)	ap-southeast-3	452118225523
Moyen-Orient (EAU) (Opt-in)	me-central-1	828603743433
Mexique (centre) Opt-in ()	mx-central-1	557690616787
Asie-Pacifique (Taïpei)	ap-east-2	863518437308
Asie-Pacifique (Nouvelle Zélande)	ap-southeast-6	686255982852
AWS GovCloud (US-East)	us-gov-east-1	226283551151
AWS GovCloud (US-West)	us-gov-west-1	226300430612

Quotas dans la protection contre les programmes malveillants pour EC2

Cette section inclut les quotas associés à l'utilisation de Malware Protection for EC2. Pour les quotas associés à GuardDuty, voir [GuardDuty quotas](#).

Le tableau suivant indique la disponibilité par défaut de diverses ressources lorsque vous utilisez Malware Protection for EC2.

Scope	Par défaut	Commentaires
Extraction et analyse des données dans un fichier compressé ou archivé	5	Nombre maximal de niveaux imbriqués autorisés dans un fichier archivé.
Nombre de fichiers contenus dans un fichier archivé	1 000	Nombre maximum de fichiers pouvant être analysés dans une archive. Ce nombre est la somme du nombre de fichiers extraits de l'archive et du nombre de fichiers extraits de toutes les archives imbriquées.
Nombre de menaces	32	Le nombre maximum de menaces que vous pouvez consulter dans le panneau des résultats. GuardDuty Malware Protection for EC2 a peut-être détecté d'autres noms de menaces. Si le nombre de noms de menaces détectées est supérieur à la valeur par défaut, vous pouvez consulter les détails JSON en sélectionnant l'ID de recherche sous le nom de la recherche dans le panneau des détails de la GuardDuty console.
Nombre de fichiers par menace détectée	5	Le nombre maximum de fichiers identifiés par menace détectée. Par exemple, si 10 fichiers associés à une

Scope	Par défaut	Commentaires
		seule menace sont GuardDuty détectés, la menace affichera un maximum de 5 fichiers.
Volumes EBS par analyse et par instance	11	Nombre maximal de volumes EBS GuardDuty pouvant être numérisés par instance EC2. Si plus de 11 volumes EBS doivent être analysés, GuardDuty Malware Protection for EC2 les trie deviceName par ordre alphabétique et sélectionne les 11 premiers volumes EBS.
Taille du volume EBS	2048 GO	Associée à une instance Amazon EC2 et à une charge de travail de conteneur, GuardDuty Malware Protection for EC2 peut scanner chaque volume Amazon EBS d'une taille maximale de 2 048 Go. Ce quota s'applique à tous ceux Région AWS où la prise en charge de Malware Protection for EC2 est disponible.

Scope	Par défaut	Commentaires
Types de système de fichiers pris en charge	<p>GuardDuty Malware Protection for EC2 peut analyser les types de systèmes de fichiers suivants :</p> <ul style="list-style-type: none"> • New Technology File System (NTFS) • X File System (XFS) • Second extended (ext2) File System • Fourth extended (ext4) File System • File Allocation Table (FAT) File System • Virtual File Allocation Table (VFAT) File System 	N/A.
Balises d'options d'analyse	50	<p>Nombre maximum de balises de ressources que vous pouvez ajouter pour personnaliser les paramètres de vos options d'analyse des logiciels malveillants. Pour plus d'informations, consultez Options d'analyse avec balises définies par l'utilisateur.</p>
Recherche de la période de conservation	90	<p>Nombre maximal de jours pendant lesquels une GuardDuty constatation est conservée. Pour obtenir les informations les plus récentes, veuillez consulter GuardDuty Quotas Amazon.</p>

Scope	Par défaut	Commentaires
Période de conservation de l'analyse des logiciels malveillants	90	Nombre maximal de jours pendant lesquels GuardDuty Malware Protection for EC2 conserve l'historique d'une analyse. Pour plus d'informations sur l'affichage des analyses des logiciels malveillants récentes, veuillez consulter Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour EC2 .
Transactions par seconde (TPS) pour l'analyse des On-demand logiciels malveillants	1	Le nombre de demandes d'analyse des On-demand programmes malveillants qui peuvent être lancées par seconde dans chaque région.
Limite de rafale pour l'analyse des On-demand logiciels malveillants	1	Nombre de demandes simultanées d'analyse des On-demand programmes malveillants qui peuvent être lancées par seconde dans chaque région.

GuardDuty Protection contre les logiciels malveillants pour S3

Malware Protection for S3 vous aide à détecter la présence potentielle de malwares en scannant les objets récemment chargés dans le bucket Amazon Simple Storage Service (Amazon S3) sélectionné. Lorsqu'un objet S3 ou une nouvelle version d'un objet S3 existant est chargé dans le compartiment que vous avez sélectionné, une analyse des programmes malveillants démarre GuardDuty automatiquement.

[Protection contre les malwares pour S3 - Présentation et démonstration](#)

Deux approches pour activer la protection contre les malwares pour S3

Vous pouvez activer Malware Protection pour S3 lorsque Compte AWS vous activez le GuardDuty service et que vous utilisez Malware Protection pour S3 dans le cadre de l' GuardDuty expérience globale, ou lorsque vous souhaitez utiliser la fonctionnalité Malware Protection pour S3 seule sans activer le GuardDuty service. Lorsque vous activez la protection contre les programmes malveillants pour S3 en tant que fonctionnalité indépendante, la GuardDuty documentation indique qu'elle utilise la protection contre les programmes malveillants pour S3 en tant que fonctionnalité indépendante.

Considérations relatives à l'utilisation indépendante de Malware Protection for S3

- GuardDuty résultats de sécurité — L'identifiant du détecteur est un identifiant unique associé à votre compte dans une région. Lorsque vous l'activez GuardDuty dans une ou plusieurs régions d'un compte, un identifiant de détecteur est créé automatiquement pour ce compte dans chaque région où vous l'activez GuardDuty. Pour plus d'informations, voir Détecteur dans le [Concepts et termes clés sur Amazon GuardDuty](#) document.

Lorsque vous activez la protection contre les programmes malveillants pour S3 indépendamment dans un compte, aucun identifiant de détecteur n'est associé à ce compte. Cela a un impact sur les GuardDuty fonctionnalités qui peuvent être mises à votre disposition. Par exemple, lorsqu'une analyse des programmes malveillants S3 détecte la présence d'un logiciel malveillant, aucun GuardDuty résultat n'est généré dans votre compte, Compte AWS car tous les GuardDuty résultats sont associés à un identifiant de détecteur.

- Vérifier si l'objet scanné est malveillant — Par défaut, GuardDuty publie les résultats de l'analyse des programmes malveillants sur votre bus d' EventBridge événements Amazon par défaut et dans un espace de CloudWatch noms Amazon. Lorsque vous activez le balisage au moment de l'activation de Malware Protection for S3 pour un compartiment, l'objet S3 scanné reçoit une balise mentionnant le résultat de l'analyse. Pour plus d'informations sur le balisage, consultez [Marquage facultatif des objets en fonction du résultat de l'analyse](#).

Considérations générales relatives à l'activation de la protection contre les programmes malveillants pour S3

Les considérations générales suivantes s'appliquent, que vous utilisiez Malware Protection pour S3 de manière indépendante ou dans le cadre de l' GuardDuty expérience :

- Vous pouvez activer la protection contre les programmes malveillants pour S3 pour un compartiment Amazon S3 appartenant à votre propre compte. En tant que compte d' GuardDuty administrateur délégué, vous ne pouvez pas activer cette fonctionnalité dans un compartiment Amazon S3 appartenant à un compte membre.
- Vous pouvez activer cette fonctionnalité dans les compartiments S3 appartenant à la même région que celle actuellement sélectionnée dans la GuardDuty console. GuardDuty ne prend pas en charge l'activation de cette fonctionnalité dans les compartiments S3 interrégionaux.
- En tant que compte d' GuardDuty administrateur délégué, vous recevrez une EventBridge notification Amazon chaque fois qu'un changement est apporté à un compartiment S3 configuré pour cette fonctionnalité par l'un des comptes membres de votre organisation. [Affichage et compréhension de l'état du compartiment protégé](#)

Table des matières

- [Tarification et coût d'utilisation de Malware Protection for S3](#)
- [Comment fonctionne Malware Protection for S3 ?](#)
- [Fonctionnalités de protection contre les malwares pour S3](#)
- [\(Facultatif\) Commencez à utiliser GuardDuty Malware Protection pour S3 de manière indépendante \(console uniquement\)](#)
- [Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket](#)
- [Étapes à suivre après avoir activé la protection contre les programmes malveillants pour S3](#)
- [On-demand Analyse des malwares S3 dans GuardDuty](#)
- [Utilisation du contrôle d'accès basé sur des balises \(TBAC\) avec Malware Protection pour S3](#)
- [Affichage et compréhension de l'état du compartiment protégé](#)
- [Surveillance des scans d'objets S3 dans Malware Protection for S3](#)
- [Résolution des problèmes](#)
- [Modification du plan de protection contre les programmes malveillants pour un compartiment protégé](#)
- [Désactivation de la protection contre les programmes malveillants pour S3 pour un compartiment protégé](#)
- [Supportabilité des fonctionnalités d'Amazon S3](#)
- [Quotas de protection contre les programmes malveillants pour S3](#)

Tarification et coût d'utilisation de Malware Protection for S3

La tarification de Malware Protection for S3 fonctionne différemment de celle des autres plans de protection GuardDuty. Alors que la plupart des plans de GuardDuty protection incluent un essai gratuit de courte durée de 30 jours, Malware Protection for S3 inclut un niveau gratuit dans AWS. Pour plus d'informations sur GuardDuty les tarifs, consultez [Tarification en GuardDuty](#).

La liste suivante indique les coûts de tarification associés à l'utilisation de Malware Protection for S3.

Niveau gratuit (coût de numérisation)

Chacun Compte AWS bénéficie d'un niveau gratuit qui inclut l'utilisation jusqu'à une limite mensuelle spécifique pour chaque région. Chacun Compte AWS bénéficie d'une utilisation mensuelle gratuite allant jusqu'à 1 000 demandes et 1 Go de données numérisées. Si votre

consommation dépasse la limite spécifiée, vous commencerez à supporter les frais d'utilisation correspondant à la limite dépassée. Pour plus de détails sur les tarifs, consultez les [tarifs GuardDuty des plans de protection](#).



Important

On-demand la numérisation n'est pas incluse dans le niveau gratuit.

Pour plus d'informations sur le coût d'utilisation après l'activation de Malware Protection pour S3, consultez [Révision du coût d'utilisation de Malware Protection for S3](#).

Coût d'utilisation du balisage d'objets S3

Lorsque vous activez la protection contre les programmes malveillants pour S3, il est facultatif d'activer le balisage pour vos objets S3 scannés. Lorsque vous choisissez d'activer le balisage d'objets S3, un coût d'utilisation est associé. Pour plus d'informations sur les coûts, consultez [l'onglet Gestion et informations](#) sur la page de tarification d'Amazon S3.

Le coût d'utilisation du balisage d'objets S3 n'est pas inclus dans le niveau gratuit.

API Amazon S3 GET et coût PUT d'utilisation

Vous devrez payer des frais d'utilisation lorsque vous GuardDuty exécuterez les API Amazon S3 en fonction du rôle IAM. Par exemple, après avoir assumé le rôle IAM, GuardDuty exécute l'PutObjectAPI pour ajouter l'objet de test au compartiment sélectionné. Cela permet GuardDuty d'évaluer le statut activé de la fonctionnalité.

Pour plus d'informations sur la tarification des appels d'API S3 dans votre Région AWS compte, consultez la section [Demandes et extraction de données sous l'onglet Stockage et demandes](#) de la page de tarification d'Amazon S3.

Le coût d'utilisation des API Amazon S3 n'est pas inclus dans le niveau gratuit.

EventBridge Coût des règles gérées

GuardDuty utilise une règle EventBridge gérée pour détecter le moment où de nouveaux objets sont chargés dans vos compartiments protégés. Vous devrez payer des frais pour les événements d'opt-in Amazon S3 ingérés par. EventBridge Vous n'aurez pas à payer de frais de livraison pour l'événement. Pour de plus amples informations sur la tarification EventBridge, consultez [Tarification EventBridge](#).

EventBridge Le coût des règles gérées n'est pas inclus dans le niveau gratuit.

Révision du coût d'utilisation de Malware Protection for S3

Votre compte commence à générer des frais d'utilisation lorsque vous utilisez Malware Protection for S3 au-delà de la limite spécifique du niveau gratuit. Pour plus d'informations sur le niveau gratuit, consultez [Tarification et coût d'utilisation de Malware Protection for S3](#). Notez que le niveau gratuit ne s'applique pas à la protection contre les programmes malveillants pour l'analyse d'objets à la demande dans S3.

La GuardDuty console ne prend pas en charge la révision du coût d'utilisation de S3 relatif à la protection contre les programmes malveillants. Pour consulter le coût d'utilisation, accédez à Cost Explorer dans la <https://console.aws.amazon.com/costmanagement/console>. Pour plus d'informations sur Compte AWS la facturation, consultez le [guide de AWS Billing l'utilisateur](#).

Pour plus d'informations sur le coût d'utilisation estimé dans GuardDuty, voir [Surveillance de l'utilisation et estimation des coûts](#).

Comment fonctionne Malware Protection for S3 ?

Cette section décrit les composants de Malware Protection for S3, son fonctionnement une fois que vous l'avez activée pour un compartiment S3 et la manière dont vous pouvez consulter l'état et le résultat de l'analyse des programmes malveillants.

Présentation de

Vous pouvez activer la protection contre les programmes malveillants pour S3 pour un compartiment Amazon S3 qui appartient au vôtre Compte AWS. GuardDuty vous permet d'activer cette fonctionnalité pour l'ensemble de votre compartiment ou de limiter la portée de l'analyse des programmes malveillants à des [préfixes d'objets](#) spécifiques, qui GuardDuty analyse le contenu de chaque objet téléchargé commençant par l'un des préfixes sélectionnés. Vous pouvez ajouter jusqu'à 5 préfixes. Lorsque vous activez la fonctionnalité pour un compartiment S3, ce compartiment est appelé compartiment protégé.

Autorisations de rôle IAM

Malware Protection for S3 utilise un rôle IAM qui permet GuardDuty d'effectuer les actions d'analyse des programmes malveillants en votre nom. Ces actions incluent le fait d'être informé des nouveaux objets téléchargés dans le compartiment sélectionné, de scanner ces objets et éventuellement d'ajouter des balises à vos objets numérisés. Il s'agit d'une condition préalable à la configuration de votre compartiment S3 avec cette fonctionnalité.

Vous avez la possibilité de mettre à jour un rôle IAM existant ou d'en créer un nouveau à cette fin. Lorsque vous activez Malware Protection for S3 pour plusieurs compartiments, vous pouvez mettre à jour le rôle IAM existant pour inclure le nom de l'autre compartiment, le cas échéant. Pour de plus amples informations, veuillez consulter [Création ou mise à jour d'une politique de rôle IAM](#).

Marquage facultatif des objets en fonction du résultat de l'analyse

Au moment d'activer Malware Protection for S3 pour votre compartiment, une étape facultative permet d'activer le balisage pour les objets S3 scannés. Le rôle IAM inclut déjà l'autorisation d'ajouter des balises à votre objet après le scan. Cependant, vous n'ajoutez des balises que si vous activez cette option au moment de la configuration.

Vous devez activer cette option avant qu'un objet ne soit chargé. Une fois le scan terminé, GuardDuty ajoute une balise prédéfinie à l'objet S3 scanné avec la paire clé:valeur suivante :

GuardDutyMalwareScanStatus:*Potential scan result*

Les valeurs potentielles des balises de résultats d'analyse incluent NO_THREATS_FOUND, THREATS_FOUND, UNSUPPORTED, ACCESS_DENIED, et FAILED. Pour plus d'informations sur ces valeurs, consultez [the section called “État du scan potentiel de l'objet S3 et état des résultats”](#).

L'activation du balisage est l'un des moyens de connaître le résultat de l'analyse des objets S3. Vous pouvez également utiliser ces balises pour ajouter une politique de ressources S3 de contrôle d'accès basé sur des balises (TBAC) afin de pouvoir prendre des mesures sur les objets potentiellement malveillants. Pour de plus amples informations, veuillez consulter [Ajouter le TBAC à la ressource du compartiment S3](#).

Nous vous recommandons d'activer le balisage au moment de configurer Malware Protection for S3 pour votre compartiment. Si vous activez le balisage après le téléchargement d'un objet et qu'il est possible que le scan soit lancé, GuardDuty vous ne pourrez pas ajouter de balises à l'objet numérisé. Pour plus d'informations sur les coûts associés au balisage d'objets S3, consultez [Tarification et coût d'utilisation de Malware Protection for S3](#).

Procédure après avoir activé la protection contre les programmes malveillants pour S3 pour un compartiment

Une fois que vous avez activé Malware Protection pour S3, une ressource de plan de protection contre les malwares est créée exclusivement pour le compartiment S3 sélectionné. Cette

ressource est associée à un identifiant de plan de protection contre les programmes malveillants, un identifiant unique pour votre ressource protégée. En utilisant l'une des autorisations IAM, GuardDuty il crée et gère une règle EventBridge gérée portant le nom de `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`.

Comment GuardDuty traite-t-on vos données ? Garde-fous pour la protection des données

Malware Protection for S3 écoute les EventBridge notifications d'Amazon. Lorsqu'un objet est chargé dans le compartiment sélectionné ou dans l'un des préfixes, GuardDuty télécharge cet objet depuis le compartiment S3 à l'aide d'un, [AWS PrivateLink](#) puis le lit, le déchiffre et le scanne dans un environnement isolé de la même région. L'environnement de numérisation s'exécute dans un cloud privé virtuel (VPC) verrouillé sans accès à Internet. Le VPC est attaché à un groupe de règles de pare-feu DNS qui autorise la communication uniquement avec les domaines autorisés qui en sont propriétaires. AWS Pendant la durée de l'analyse, stocke GuardDuty temporairement l'objet S3 téléchargé dans l'environnement d'analyse chiffré à l'aide des clés [AWS Key Management Service \(AWS KMS\)](#).

Note

Par défaut, toutes les API Amazon S3 répertoriées sous le [type d'événement créé par un objet](#) dans le guide de l'utilisateur Amazon S3 lanceront le scan de protection contre les programmes malveillants pour S3.

Ces types d'événements incluent [PutObjectCopyObject](#), [objet POST](#) et [CompleteMultipartUpload](#).

Pour plus d'informations sur la méthodologie de détection des GuardDuty programmes malveillants et les moteurs d'analyse qu'elle utilise, consultez [GuardDuty moteur d'analyse pour la détection des malwares](#).

Une fois l'analyse des programmes malveillants terminée, GuardDuty traite les métadonnées de l'analyse avec l'état de l'analyse, puis supprime la copie téléchargée de l'objet.

GuardDuty nettoie l'environnement de numérisation à chaque fois avant le début d'une nouvelle analyse. GuardDuty utilise une autorisation conditionnelle pour l'accès des opérateurs à l'environnement de numérisation, et chaque demande d'accès est examinée, approuvée et auditée.

Révision de l'état et du résultat de l'analyse des objets S3

GuardDuty publie l'événement du résultat de l'analyse des objets S3 dans le bus d'événements EventBridge par défaut d'Amazon. GuardDuty envoie également les mesures de numérisation telles que le nombre d'objets scannés et le nombre d'octets scannés à Amazon CloudWatch. Si vous avez activé le balisage, vous GuardDuty ajouterez la balise prédéfinie GuardDutyMalwareScanStatus et un résultat de numérisation potentiel en tant que valeur de balise.

Important

GuardDuty utilise la livraison au moins une fois, ce qui signifie que vous pouvez recevoir plusieurs résultats de numérisation pour le même objet. Nous vous recommandons de concevoir vos applications de manière à gérer les résultats dupliqués. Vous n'êtes facturé qu'une seule fois pour chaque objet numérisé.

Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 dans Malware Protection for S3](#).

Révision des résultats générés

L'examen des résultats dépend de l'utilisation ou non de Malware Protection for S3 avec GuardDuty. Réfléchissez aux scénarios suivants :

Utilisation de la protection contre les programmes malveillants pour S3 lorsque le GuardDuty service est activé (ID du détecteur)

Si l'analyse des programmes malveillants détecte un fichier potentiellement malveillant dans un objet S3, elle GuardDuty générera un résultat associé. Vous pouvez consulter les détails de la recherche et suivre les étapes recommandées pour éventuellement y remédier. En fonction de la [fréquence de vos résultats d'exportation](#), les résultats générés sont exportés vers un compartiment S3 et un bus EventBridge d'événements.

Pour plus d'informations sur le type de recherche qui serait généré, consultez [Protection contre les programmes malveillants pour le type de recherche S3](#).

Utilisation de Malware Protection pour S3 en tant que fonctionnalité indépendante (aucun identifiant de détecteur)

GuardDuty ne sera pas en mesure de générer des résultats car aucun identifiant de détecteur n'est associé. Pour connaître l'état de l'analyse des malwares sur les objets S3, vous pouvez

consulter le résultat de l'analyse qui est GuardDuty automatiquement publié sur votre bus d'événements par défaut. Vous pouvez également consulter les CloudWatch mesures pour évaluer le nombre d'objets et d'octets qui GuardDuty ont été tentés de scanner. Vous pouvez configurer des CloudWatch alarmes pour être informé des résultats de l'analyse. Si vous avez activé le balisage des objets S3, vous pouvez également consulter l'état de l'analyse des programmes malveillants en vérifiant la clé de balise et la valeur de la GuardDutyMalwareScanStatus balise de résultat de l'analyse dans l'objet S3.

Pour plus d'informations sur l'état et le résultat de l'analyse des objets S3, consultez [Surveillance des scans d'objets S3 dans Malware Protection for S3](#).

Fonctionnalités de protection contre les malwares pour S3

La liste suivante fournit un aperçu de ce à quoi vous pouvez vous attendre ou de ce que vous pouvez faire après avoir activé Malware Protection for S3 pour votre compartiment :

- Choisissez les éléments à analyser : scannez les fichiers au fur et à mesure qu'ils sont chargés dans tous les préfixes ou dans des préfixes spécifiques (jusqu'à 5) associés au compartiment S3 que vous avez sélectionné.
- Analyses automatiques des objets chargés : une fois que vous avez activé la protection contre les programmes malveillants pour S3 pour un compartiment, une analyse est GuardDuty automatiquement lancée pour détecter les logiciels malveillants potentiels dans un objet récemment chargé.
- On-demand scans : vous pouvez lancer des scans pour des objets existants ou numériser à nouveau des objets précédemment numérisés. Pour de plus amples informations, veuillez consulter [On-demand Analyse des malwares S3 dans GuardDuty](#).
- Activez via la console, à l'aide de l'API/AWS CLI, ou CloudFormation — Choisissez une méthode préférée pour activer la protection contre les logiciels malveillants pour S3.

Vous pouvez activer la protection contre les programmes malveillants pour S3 en utilisant des plateformes d'infrastructure en tant que code (IaC) telles que Terraform. Pour plus d'informations, voir [Ressource : aws_guardduty_malware_protection_plan](#).

- Formats de fichiers pris en charge, protection contre les programmes malveillants pour les quotas S3 et fonctionnalités Amazon S3 : Malware Protection for S3 prend en charge tous les formats de fichiers que vous pouvez télécharger dans un compartiment S3. Si le fichier téléchargé est protégé par mot de passe et GuardDuty est capable de détecter la présence d'une protection par mot de

pour le type de fichier téléchargé, il GuardDuty essaiera de scanner le contenu d'origine à l'aide de mots de passe courants. Si le mot de passe échoue, le scan sera ignoré. GuardDuty Impossible de détecter la présence d'une protection par mot de passe sur tous les formats de fichiers. S'il n'est pas GuardDuty possible de détecter la présence d'une protection par mot de passe, le contenu chiffré GuardDuty sera tout de même scanné.

Pour plus d'informations sur les quotas liés à la taille des objets, au niveau de profondeur d'archivage maximal et pour d'autres informations, consultez [Quotas de protection contre les programmes malveillants pour S3](#).

Pour savoir si une fonctionnalité Amazon S3 est prise en charge ou non, consultez [Supportabilité des fonctionnalités d'Amazon S3](#).

- Prend en charge le balisage des objets S3 scannés : lorsque vous activez [Marquage facultatif des objets en fonction du résultat de l'analyse](#), une balise indiquant l'état de l'analyse est ajoutée après chaque analyse de logiciels malveillants. GuardDuty Vous pouvez utiliser cette balise pour configurer le contrôle d'accès basé sur les balises (TBAC) pour les objets S3. Par exemple, vous pouvez restreindre l'accès aux objets S3 indiqués comme malveillants et dont la valeur de balise est égale à THREATS_FOUND.
- EventBridge Notifications Amazon : GuardDuty envoie des événements à Amazon EventBridge lorsque le statut des ressources du plan de protection contre les malwares change ou lorsqu'une analyse des programmes malveillants de l'objet S3 est terminée. Ces événements sont envoyés au bus d'événements par défaut. Vous pouvez utiliser EventBridge ces événements pour écrire des règles qui prennent des mesures, telles que la surveillance lorsque ces événements se produisent. Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).
- CloudWatch métriques — Consultez CloudWatch les métriques pour activer les alarmes lors de l'état de certains programmes malveillants. Pour de plus amples informations, veuillez consulter [Métriques d'état d'analyse des objets S3 dans CloudWatch](#).

(Facultatif) Commencez à utiliser GuardDuty Malware Protection pour S3 de manière indépendante (console uniquement)

Utilisez cette étape facultative lorsque vous souhaitez commencer à utiliser l'option de détection des menaces Malware Protection for S3 indépendamment de l'état de votre Compte AWS.

Si vous souhaitez également utiliser d'autres plans de protection dédiés GuardDuty, vous devez commencer par utiliser le GuardDuty service Amazon. Pour plus d'informations sur les plans de GuardDuty protection, consultez [Caractéristiques de GuardDuty](#). Lorsque vous l'avez déjà activée GuardDuty dans votre compte, vous pouvez ignorer cette étape et continuer [Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket](#).

Étapes pour démarrer avec Malware Protection pour la détection des menaces uniquement dans S3

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Sélectionnez GuardDuty Malware Protection pour S3 uniquement. Cela vous permet de détecter si un fichier récemment chargé dans votre compartiment Amazon Simple Storage Service (Amazon S3) contient potentiellement un logiciel malveillant.

Try threat detection with GuardDuty

- ☐ Amazon GuardDuty - all features
Experience threat detection capabilities in your AWS environment.
- ☒ **GuardDuty Malware Protection for S3 only**
Detect malicious file upload to your Amazon S3 buckets. You don't need to enable Amazon GuardDuty.

Get started

3. Choisissez Démarrer. Vous pouvez maintenant suivre les étapes ci-dessous [Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket](#).

Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket

Pour que Malware Protection for S3 puisse analyser et (éventuellement) ajouter des balises à vos objets S3, vous pouvez utiliser des rôles de service dotés des autorisations nécessaires pour effectuer des actions d'analyse des programmes malveillants en votre nom. Pour plus d'informations sur l'utilisation des rôles de service pour activer la protection contre les programmes malveillants pour S3, consultez [Service Access](#). Ce rôle est différent du rôle lié au service [GuardDuty Malware Protection](#).

Si vous préférez utiliser les rôles IAM, vous pouvez associer un rôle IAM qui inclut les autorisations requises pour scanner et (éventuellement) ajouter des balises à vos objets S3. GuardDuty assume ensuite ce rôle IAM pour effectuer ces actions en votre nom. Vous aurez besoin de ce nom de rôle IAM au moment de l'activation de ce plan de protection pour votre compartiment Amazon S3.

Si vous utilisez des rôles IAM, chaque fois que vous souhaitez protéger un compartiment Amazon S3, vous devez suivre les deux étapes répertoriées dans cette section.

Pour activer la protection contre les programmes malveillants pour S3, vous aurez besoin de détails tels que le nom du compartiment S3, les préfixes d'objets si vous souhaitez concentrer la protection sur des préfixes spécifiques, et le nom du rôle IAM avec les autorisations requises.

Les étapes restent les mêmes, que vous commenciez à utiliser Malware Protection pour S3 de manière indépendante ou que vous l'activiez dans le cadre du GuardDuty service.

Rubriques

1. [Création ou mise à jour d'une politique de rôle IAM](#)
2. [Activation de la protection contre les programmes malveillants pour S3 pour votre bucket](#)
3. [Résolution d'une erreur d'autorisation de rôle IAM](#)

Activation de la protection contre les programmes malveillants pour S3 pour votre bucket

Cette section explique en détail comment activer la protection contre les programmes malveillants pour S3 pour un compartiment dans votre propre compte. Avant de poursuivre, prenez en compte les points suivants :

- Lorsque vous activez ce plan de protection à l'aide de la GuardDuty console, il inclut l'étape permettant de créer un nouveau rôle ou d'utiliser un rôle existant dans la section Accès au service.
- Lorsque vous activez ce plan de protection à l'aide de l' GuardDuty API ou de l'interface de ligne de commande, vous devez [Création ou mise à jour d'une politique de rôle IAM](#) le faire avant de poursuivre.
- Quelle que soit la manière dont vous activez ce plan de protection, vous devez disposer des éléments requis [Autorisations pour créer une ressource de plan de protection contre les programmes malveillants](#).

Prise en compte de la limitation des compartiments Amazon S3

S3 Throttling peut limiter la vitesse à laquelle les données peuvent être transférées depuis ou vers vos compartiments Amazon S3. Cela peut potentiellement retarder les analyses malveillantes de vos objets récemment chargés.

Si vous vous attendez à recevoir des volumes GET et des PUT demandes élevés dans vos compartiments S3, envisagez de mettre en œuvre des mesures pour empêcher la limitation.

Pour plus d'informations sur la manière de procéder, consultez la section [Empêcher la limitation d'Amazon S3](#) dans le guide de l'utilisateur d'Amazon Athena.

Autorisations pour créer une ressource de plan de protection contre les programmes malveillants

Lorsque vous activez la protection contre les programmes malveillants pour S3 pour un compartiment Amazon S3, vous GuardDuty créez une ressource de plan de protection contre les programmes malveillants qui sert d'identifiant pour le plan de protection du compartiment. Si vous n'utilisez pas encore le [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#), vous devez ajouter les autorisations suivantes pour créer cette ressource :

- `guardDuty:CreateMalwareProtectionPlan`
- `iam:PassRole`

Vous pouvez utiliser l'exemple de politique personnalisée suivant et le *placeholder values* remplacer par les valeurs appropriées à votre compte :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/role-name",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateMalwareProtectionPlan"
      ],
      "Resource": "*"
    }
  ]
}
```

Activation de la protection contre les programmes malveillants pour S3 à l'aide de GuardDuty la console

Les sections suivantes proposent une procédure pas à pas, telle que vous la découvrirez dans la GuardDuty console.

Pour activer la protection contre les programmes malveillants pour S3 à l'aide de GuardDuty la console

Entrez les détails du compartiment S3

Procédez comme suit pour fournir les informations relatives au compartiment Amazon S3 :

1. Connectez-vous à Console de gestion AWS et ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez activer la protection contre les programmes malveillants pour S3.
3. Dans le volet de navigation, choisissez **Malware Protection pour S3**.
4. Dans la section **Compartiments protégés**, choisissez **Activer** pour activer la protection contre les programmes malveillants pour S3 pour un compartiment S3 qui appartient au vôtre. **Compte AWS**
5. Dans **Entrez les détails du compartiment S3**, entrez le **nom du compartiment Amazon S3**. Vous pouvez également choisir **Browse S3** pour sélectionner un compartiment S3.

L'emplacement Région AWS du compartiment S3 et l' **Compte AWS** endroit où vous activez la protection contre les programmes malveillants pour S3 doivent être identiques. Par exemple, si votre compte appartient à la **us-east-1** région, la région de votre compartiment Amazon S3 doit également l'être **us-east-1**.

6. Sous **Préfixe**, vous pouvez sélectionner **Tous les objets du compartiment S3** ou **Objets commençant par un préfixe spécifique**.
 - Sélectionnez **Tous les objets du compartiment S3** lorsque vous le souhaitez GuardDuty pour numériser tous les objets récemment chargés dans le compartiment sélectionné.
 - Sélectionnez **Objets commençant par un préfixe spécifique** lorsque vous souhaitez scanner les objets récemment chargés qui appartiennent à un préfixe spécifique. Cette option vous permet de concentrer la portée de l'analyse des programmes malveillants sur les préfixes d'objets sélectionnés uniquement. Pour plus d'informations sur l'utilisation des préfixes, consultez la section [Organisation des objets dans la console Amazon S3 à l'aide de dossiers](#) dans le guide de l'utilisateur Amazon S3.

Choisissez **Ajouter un préfixe** et saisissez le préfixe. Vous pouvez ajouter jusqu'à cinq préfixes.

Activer le balisage pour les objets numérisés

Il s'agit d'une étape facultative. Lorsque vous activez l'option de marquage avant qu'un objet ne soit chargé dans votre compartiment, une fois l'analyse terminée, GuardDuty une balise prédéfinie est ajoutée avec la touche « as » **GuardDutyMalwareScanStatus** et la valeur comme résultat de

l'analyse. Pour utiliser de manière optimale Malware Protection for S3, nous vous recommandons d'activer l'option permettant d'ajouter une balise aux objets S3 une fois l'analyse terminée. Le coût standard du balisage des objets S3 s'applique. Pour de plus amples informations, veuillez consulter [Tarification et coût d'utilisation de Malware Protection for S3](#).

Pourquoi devriez-vous activer le balisage ?

- L'activation du balisage est l'un des moyens de connaître le résultat de l'analyse des programmes malveillants. Pour plus d'informations sur le résultat d'une analyse de programmes malveillants S3, consultez [Surveillance des scans d'objets S3 dans Malware Protection for S3](#).
- Configurez une politique de contrôle d'accès basé sur les balises (TBAC) sur votre compartiment S3 qui contient l'objet potentiellement malveillant. Pour plus d'informations sur les considérations à prendre en compte et sur la manière de mettre en œuvre le contrôle d'accès basé sur les balises (TBAC), consultez. [Utilisation du contrôle d'accès basé sur des balises \(TBAC\) avec Malware Protection pour S3](#)

Considérations relatives GuardDuty à l'ajout d'une balise à votre objet S3 :

- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet. Pour plus d'informations, consultez la section [Catégorisation de votre stockage à l'aide de balises](#) dans le guide de l'utilisateur Amazon S3.

Si les 10 balises sont déjà utilisées, impossible GuardDuty d'ajouter la balise prédéfinie à l'objet numérisé. GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).

- Lorsque le rôle IAM sélectionné n'inclut pas l'autorisation de GuardDuty baliser l'objet S3, même si le balisage est activé pour votre compartiment protégé, vous ne GuardDuty pourrez pas ajouter de balise à cet objet S3 scanné. Pour plus d'informations sur l'autorisation de rôle IAM requise pour le balisage, consultez. [Création ou mise à jour d'une politique de rôle IAM](#)

GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).

Pour sélectionner une option sous Marquer les objets numérisés

- Lorsque vous souhaitez ajouter GuardDuty des balises à vos objets S3 numérisés, sélectionnez Marquer les objets.
- Si vous ne souhaitez pas ajouter GuardDuty de balises à vos objets S3 numérisés, sélectionnez Ne pas baliser les objets.

Accès au service

Procédez comme suit pour choisir un rôle de service existant ou créer un nouveau rôle de service doté des autorisations nécessaires pour effectuer des actions d'analyse des programmes malveillants en votre nom. Ces actions peuvent inclure l'analyse des objets S3 récemment chargés et (éventuellement) l'ajout de balises à ces objets. Pour plus d'informations sur les autorisations dont bénéficiera ce rôle, consultez [Création ou mise à jour d'une politique de rôle IAM](#).

Dans la section Accès au service, vous pouvez effectuer l'une des opérations suivantes :

1. Créer et utiliser un nouveau rôle de service — Vous pouvez créer un nouveau rôle de service doté des autorisations nécessaires pour effectuer une analyse des programmes malveillants.

Sous le nom du rôle, vous pouvez choisir d'utiliser le nom prérempli par GuardDuty ou de saisir un nom significatif de votre choix pour identifier le rôle. Par exemple GuardDutyS3MalwareScanRole. Le nom du rôle doit comprendre de 1 à 64 caractères. Les caractères valides sont les caractères a-z A-Z, 0-9 et les caractères « +=, .@-_ ».
2. Utiliser un rôle de service existant : vous pouvez choisir un rôle de service existant dans la liste des noms des rôles de service.
 - a. Sous Modèle de politique, vous pouvez consulter la politique de votre compartiment S3. Assurez-vous d'avoir saisi ou sélectionné un compartiment S3 dans la section Entrez les détails du compartiment S3.
 - b. Sous Nom du rôle de service, choisissez un rôle de service dans la liste des rôles de service.

Vous pouvez modifier la politique en fonction de vos besoins. Pour plus de détails sur la manière de créer ou de mettre à jour un rôle IAM, voir [Créer ou mettre à jour une politique de rôle IAM](#).

Pour les problèmes liés aux autorisations de rôle IAM, consultez [Résolution d'une erreur d'autorisation de rôle IAM](#).

(Facultatif) Marquer l'ID du plan de protection contre les programmes malveillants

Il s'agit d'une étape facultative qui vous permet d'ajouter des balises à la ressource du plan de protection contre les programmes malveillants qui serait créée pour votre ressource de compartiment S3.

Chaque balise comporte deux parties : une clé de balise et une valeur de balise facultative. Pour plus d'informations sur le balisage et ses avantages, consultez la section Ressources de [balisage. AWS](#)

Pour ajouter des balises à la ressource de votre plan de protection contre les programmes malveillants

1. Entrez la clé et une valeur facultative pour la balise. La clé de balise et la valeur de la balise distinguent les majuscules et minuscules. Pour plus d'informations sur les noms de la clé et de la valeur de la balise, voir Limites et exigences en matière de dénomination des [balises](#).
2. Pour ajouter d'autres balises à la ressource de votre plan de protection contre les programmes malveillants, choisissez Ajouter une nouvelle étiquette et répétez l'étape précédente. Vous pouvez ajouter jusqu'à 50 balises à chaque ressource .
3. Sélectionnez Activer.

Activation de la protection contre les programmes malveillants pour S3 à l'aide de API/CLI

Cette section décrit les étapes à suivre pour activer la protection contre les programmes malveillants pour S3 par programmation dans votre AWS environnement. Cela nécessite le rôle IAM Amazon Resource Name (ARN) que vous avez créé au cours de cette étape -[Création ou mise à jour d'une politique de rôle IAM](#).

Pour activer la protection contre les programmes malveillants pour S3 par programmation à l'aide de API/CLI

- En utilisant l'API

Exécutez le [CreateMalwareProtectionPlan](#) pour activer la protection contre les programmes malveillants pour S3 pour un compartiment appartenant à votre propre compte.

- En utilisant AWS CLI

Selon la manière dont vous souhaitez activer la protection contre les programmes malveillants pour S3, la liste suivante fournit des AWS CLI exemples de commandes pour un cas d'utilisation

spécifique. Lorsque vous exécutez ces commandes, remplacez le *placeholder examples shown in red*, par les valeurs appropriées à votre compte.

AWS CLI exemples de commandes

- Utilisez la AWS CLI commande suivante pour activer la protection contre les programmes malveillants pour S3 pour un compartiment sans balisage pour les objets S3 scannés :

```
aws guardduty create-malware-protection-plan --role  
"arn:aws:iam::<111122223333:role/role-name" --protected-resource  
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Utilisez la AWS CLI commande suivante pour activer la protection contre les programmes malveillants pour S3 pour un compartiment comportant des préfixes d'objets spécifiques et aucun balisage pour les objets S3 scannés :

```
aws guardduty create-malware-protection-plan --role  
"arn:aws:iam::<111122223333:role/role-name" --protected-resource '{"S3Bucket":  
{"BucketName":"amzn-s3-demo-bucket1", "ObjectPrefixes": ["Object1", "Object1"]}}'
```

- Utilisez la AWS CLI commande suivante pour activer la protection contre les programmes malveillants pour S3 pour un compartiment dans lequel le balisage des objets S3 scannés est activé :

```
aws guardduty create-malware-protection-plan --role  
"arn:aws:iam::<111122223333:role/role-name" --protected-resource  
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"} --actions  
"Tagging"={"Status"="ENABLED"}
```

Une fois ces commandes exécutées avec succès, un identifiant de plan de protection contre les programmes malveillants unique sera généré. Pour effectuer des actions telles que la mise à jour ou la désactivation du plan de protection de votre compartiment, vous aurez besoin de cet identifiant de plan de protection contre les programmes malveillants.

Pour les problèmes liés aux autorisations de rôle IAM, consultez [Résolution d'une erreur d'autorisation de rôle IAM](#).

Création ou mise à jour d'une politique de rôle IAM

Pour que Malware Protection for S3 puisse analyser et (éventuellement) ajouter des balises à vos objets S3, vous pouvez utiliser des rôles de service dotés des autorisations nécessaires pour effectuer des actions d'analyse des programmes malveillants en votre nom. Pour plus d'informations sur l'utilisation des rôles de service pour activer la protection contre les programmes malveillants pour S3, consultez [Service Access](#). Ce rôle est différent du rôle lié au service [GuardDuty Malware Protection](#).

Si vous préférez utiliser les rôles IAM, vous pouvez associer un rôle IAM qui inclut les autorisations requises pour scanner et (éventuellement) ajouter des balises à vos objets S3. Vous devez créer un rôle IAM ou mettre à jour un rôle existant pour inclure ces autorisations. Ces autorisations étant requises pour chaque compartiment Amazon S3 pour lequel vous activez Malware Protection for S3, vous devez effectuer cette étape pour chaque compartiment Amazon S3 que vous souhaitez protéger.

La liste suivante explique comment certaines autorisations permettent d' GuardDuty effectuer l'analyse des programmes malveillants en votre nom :

- Autorisez Amazon EventBridge Actions à créer et à gérer la règle EventBridge gérée afin que Malware Protection for S3 puisse écouter les notifications de vos objets S3.

Pour plus d'informations, consultez les règles EventBridge gérées par [Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

- Autoriser Amazon S3 et EventBridge les actions à envoyer des notifications EventBridge pour tous les événements de ce compartiment

Pour plus d'informations, consultez la section [Activation d'Amazon EventBridge](#) dans le guide de l'utilisateur Amazon S3.

- Autorisez les actions Amazon S3 à accéder à l'objet S3 chargé et ajoutez une balise prédéfinie à l'objet S3 numérisé. GuardDutyMalwareScanStatus Lorsque vous utilisez un préfixe d'objet, ajoutez une `s3:prefix` condition sur les préfixes ciblés uniquement. Cela vous GuardDuty empêche d'accéder à tous les objets S3 de votre compartiment.
- Autorisez les actions clés KMS à accéder à l'objet avant de numériser et de placer un objet de test dans des compartiments avec le SSE-KMS cryptage pris DSSE-KMS en charge.

 Note

Cette étape est requise chaque fois que vous activez la protection contre les programmes malveillants pour S3 pour un compartiment de votre compte. Si vous possédez déjà un rôle IAM, vous pouvez mettre à jour sa politique pour inclure les détails d'une autre ressource de compartiment Amazon S3. La [Ajouter des autorisations de politique IAM](#) rubrique fournit un exemple sur la manière de procéder.

Utilisez les politiques suivantes pour créer ou mettre à jour un rôle IAM.

Stratégies

- [Ajouter des autorisations de politique IAM](#)
- [Ajouter une politique de relation de confiance](#)

Ajouter des autorisations de politique IAM

Vous pouvez choisir de mettre à jour la politique en ligne d'un rôle IAM existant ou de créer un nouveau rôle IAM. Pour plus d'informations sur les étapes, consultez [Création d'un rôle IAM](#) ou [Modification de la politique d'autorisations d'un rôle](#) dans le Guide de l'utilisateur IAM.

Ajoutez le modèle d'autorisations suivant à votre rôle IAM préféré. Remplacez les valeurs d'espace réservé suivantes par les valeurs appropriées associées à votre compte :

- Par *amzn-s3-demo-bucket*, remplacez-le par le nom de votre compartiment Amazon S3.

Pour utiliser le même rôle IAM pour plusieurs ressources de compartiment S3, mettez à jour une politique existante comme indiqué dans l'exemple suivant :

```
...  
...  
"Resource": [  
    "arn:aws:s3:::amzn-s3-demo-bucket/*",  
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"  
],  
...  
...
```

Assurez-vous d'ajouter une virgule (,) avant d'ajouter un nouvel ARN associé au compartiment S3. Effectuez cette opération chaque fois que vous faites référence à un compartiment S3 Resource dans le modèle de politique.

- Pour **111122223333**, remplacez-le par votre Compte AWS identifiant.
- Pour **us-east-1**, remplacez-le par votre Région AWS.
- Pour **APKAEIBAERJR2EXAMPLE**, remplacez-le par votre identifiant de clé géré par le client. Si votre compartiment S3 est chiffré à l'aide d'une AWS KMS clé, nous ajoutons les autorisations pertinentes si vous choisissez l'[option](#) Créer un nouveau rôle lors de la configuration de la protection contre les programmes malveillants pour votre compartiment.

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

Modèle de politique de rôle IAM

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
      "Effect": "Allow",
      "Action": [
        "events:PutRule",
        "events>DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource": [
        "arn:aws:events:us-east-1:111122223333:rule/D0-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
      ],
      "Condition": {
        "StringLike": {
          "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
  "Effect": "Allow",
  "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource": [
    "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
  ]
},
{
  "Sid": "AllowPostScanTag",
  "Effect": "Allow",
  "Action": [
    "s3:PutObjectTagging",
    "s3:GetObjectTagging",
    "s3:PutObjectVersionTagging",
    "s3:GetObjectVersionTagging"
  ],
  "Resource": [
    "arn:aws:s3::amzn-s3-demo-bucket/*"
  ]
},
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3::amzn-s3-demo-bucket"
  ]
},
{
  "Sid": "AllowPutValidationObject",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
```

```

        "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-
validation-object"
    ],
    {
        "Sid": "AllowCheckBucketOwnership",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "AllowMalwareScan",
        "Effect": "Allow",
        "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "AllowDecryptForMalwareScan",
        "Effect": "Allow",
        "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-
east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "s3.us-east-1.amazonaws.com"
            }
        }
    }
]
}

```

Ajouter une politique de relation de confiance

Associez la politique de confiance suivante à votre rôle IAM. Pour plus d'informations sur les étapes à suivre, consultez [la section Modification d'une politique de confiance relative aux rôles](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Résolution d'une erreur d'autorisation de rôle IAM

Lorsque vous activez Malware Protection pour S3, GuardDuty vérifiez si votre rôle de service IAM dispose des autorisations nécessaires pour valider la propriété du compartiment Amazon S3. Si ces autorisations sont manquantes ou mal configurées, le message suivant peut s'afficher :

```
"message": "The request was rejected because provided IAM role does not have the
required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Les scénarios suivants peuvent vous aider à résoudre cette erreur :

Autorisations de rôle IAM manquantes

- Le rôle IAM doit disposer des autorisations requises pour permettre à Malware Protection for S3 d'assumer le rôle.
- GuardDuty valide la propriété du bucket avec l'"s3:ListBucket" autorisation. Cela doit être présent dans le rôle IAM que vous utilisez.

Pour plus d'informations sur les autorisations, consultez [Création ou mise à jour d'une politique de rôle IAM](#).

Disponibilité des rôles IAM

- Lorsque vous créez un nouveau rôle IAM, attendez quelques minutes pour que les modifications soient finalement cohérentes avant d'activer Malware Protection pour S3. Si vous essayez d'activer le plan de protection immédiatement après avoir créé le rôle, la validation risque d'échouer.
- Pour les déploiements d'infrastructure en tant que code (IaC), il est GuardDuty recommandé de déclarer une dépendance aux ressources afin de garantir la cohérence finale du rôle IAM.

Pour des exemples de modèles expliquant comment procéder, consultez le [GuardDuty GitHub référentiel](#).

Cross-region habilitation

Assurez-vous que votre compartiment Amazon S3 se trouve dans la même région que celle dans laquelle vous activez la protection contre les programmes malveillants pour S3 GuardDuty.

Étapes à suivre après avoir activé la protection contre les programmes malveillants pour S3

Cette section répertorie les étapes que vous pouvez suivre après avoir activé Malware Protection for S3 pour un compartiment. Les étapes suivantes sont répertoriées dans un ordre qui vous aidera à passer aux étapes suivantes :

À suivre après avoir activé la protection contre les programmes malveillants pour S3 pour votre compartiment

1. Ajouter une politique de ressources de contrôle d'accès basée sur des balises (TBAC) : lorsque vous activez le balisage, assurez-vous d'ajouter la politique TBAC à la ressource de votre compartiment S3 avant qu'un objet ne soit chargé dans le compartiment sélectionné. Pour de plus amples informations, veuillez consulter [Ajouter le TBAC à la ressource du compartiment S3](#).
2. Surveiller l'état du plan de protection contre les programmes malveillants : surveillez la colonne État de chaque compartiment protégé. Pour plus d'informations sur les statuts potentiels et leur signification, consultez [Affichage et compréhension de l'état du compartiment protégé](#).
3. Lancez une analyse en choisissant l'une des options suivantes :
 - Téléchargez un objet :

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Téléchargez un fichier dans le compartiment S3 ou dans le préfixe d'objet pour lequel vous avez activé cette fonctionnalité. Pour savoir comment charger un fichier, consultez la section [Charger un objet dans votre compartiment](#) dans le guide de l'utilisateur Amazon S3.
- Lancez une analyse à la demande : [On-demand Analyse des malwares S3 dans GuardDuty](#)
4. Surveiller l'état de l'analyse des objets S3 et les résultats de l'analyse : cette étape inclut des informations sur la façon de vérifier l'état de l'analyse des programmes malveillants de l'objet S3.

Activé à la fois GuardDuty et protection contre les logiciels malveillants pour S3	Protection contre les programmes malveillants activée pour S3 uniquement
<ul style="list-style-type: none"> Lorsqu'il GuardDuty est activé, il peut générer le Protection contre les programmes malveillants pour le type de recherche S3 pour indiquer la présence d'un logiciel malveillant dans l'objet S3 scanné. Vous pouvez éventuellement vérifier le résultat de l'analyse des objets S3 en utilisant une ou plusieurs options ci-dessous Surveillance des scans d'objets S3 dans Malware Protection for S3. Il s'agit notamment de l'utilisation d'Amazon EventBridge, CloudWatch des métriques pour le plan de protection contre les logiciels malveillants et du marquage des objets numérisés. 	<p>Vous pouvez éventuellement vérifier le résultat de l'analyse des objets S3 en utilisant une ou plusieurs options ci-dessous Surveillance des scans d'objets S3 dans Malware Protection for S3. Il s'agit notamment de l'utilisation d'Amazon EventBridge, CloudWatch des métriques pour le plan de protection contre les logiciels malveillants et du marquage des objets numérisés.</p>

On-demand Analyse des malwares S3 dans GuardDuty

GuardDuty Malware Protection for S3 surveille en permanence les nouveaux téléchargements S3. Pour les objets qui existaient avant l'activation de la protection, ou pour réanalyser des objets précédemment analysés, vous pouvez lancer une analyse des programmes malveillants S3 à la demande une fois que vous avez activé le plan de protection contre les GuardDuty programmes malveillants pour votre compartiment.

On-demand l'analyse des programmes malveillants utilise le rôle IAM du plan de protection contre les programmes malveillants pour l'accès aux objets et l'application de la configuration. L'analyse remplacera tout préfixe configuré dans le plan de protection contre les programmes malveillants pour le compartiment.

Note

Le quota Malware Protection for S3 s'applique à l'analyse des programmes malveillants à la demande. Pour plus d'informations, voir [Quotas de protection contre les programmes malveillants pour S3](#).

Pour de plus amples informations sur la tarification, consultez [Tarification et coût d'utilisation de Malware Protection for S3](#).

Conditions préalables

Avant de lancer une analyse des programmes malveillants à la demande, votre compte doit remplir les conditions préalables suivantes :

- La protection contre les programmes malveillants pour S3 est activée sur le compartiment cible. Pour plus d'informations, consultez [Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket](#).
- La [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) politique est attachée à l'utilisateur IAM ou au rôle IAM qui appelle l'API.

Lancer une analyse des programmes malveillants à la

Utilisez l'opération [SendObjectMalwareScan](#) API, qui nécessite le chemin de l'objet S3 en entrée.

API/CLI

Vous pouvez numériser la dernière version de l'objet ou spécifier une version particulière à numériser.

Pour scanner une version spécifique d'un objet :

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket":  
  "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE", "VersionId":  
  "d41d8cd98f00b204e9800998eEXAMPLE"}'
```

Pour scanner la dernière version d'un objet :

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket": "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE"}'
```

Important

Un appel d'API réussi confirme que la demande d'analyse a été acceptée. Cependant, il est important de surveiller les résultats de l'analyse pour garantir le bon déroulement de l'analyse et identifier les éventuels problèmes, tels que les erreurs d'accès à l'objet. Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 dans Malware Protection for S3](#).

Utilisation du contrôle d'accès basé sur des balises (TBAC) avec Malware Protection pour S3

Lorsque vous activez Malware Protection for S3 pour votre compartiment, vous pouvez éventuellement choisir d'activer le balisage. Après avoir tenté de scanner un objet S3 récemment chargé dans le compartiment sélectionné, GuardDuty ajoute une balise à l'objet scanné pour indiquer l'état de l'analyse des programmes malveillants. Un coût d'utilisation direct est associé à l'activation du balisage. Pour de plus amples informations, veuillez consulter [Tarification et coût d'utilisation de Malware Protection for S3](#).

GuardDuty utilise une balise prédéfinie avec la clé as GuardDutyMalwareScanStatus et la valeur comme l'un des statuts d'analyse des programmes malveillants. Pour plus d'informations sur ces valeurs, consultez [the section called “État du scan potentiel de l'objet S3 et état des résultats”](#).

Considérations relatives GuardDuty à l'ajout d'une balise à votre objet S3 :

- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet. Pour plus d'informations, consultez la section [Catégorisation de votre stockage à l'aide de balises](#) dans le guide de l'utilisateur Amazon S3.

Si les 10 balises sont déjà utilisées, GuardDuty vous ne pouvez pas ajouter la balise prédéfinie à l'objet numérisé. GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge

événements par défaut. Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).

- Lorsque le rôle IAM sélectionné n'inclut pas l'autorisation de GuardDuty baliser l'objet S3, même si le balisage est activé pour votre compartiment protégé, vous ne pouvez pas ajouter de balise à cet objet S3 scanné. Pour plus d'informations sur l'autorisation de rôle IAM requise pour le balisage, consultez [Création ou mise à jour d'une politique de rôle IAM](#)

GuardDuty publie également le résultat de l'analyse sur votre bus d'EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).

Ajouter le TBAC à la ressource du compartiment S3

Vous pouvez utiliser les politiques de ressources du compartiment S3 pour gérer le contrôle d'accès basé sur les balises (TBAC) pour vos objets S3. Vous pouvez autoriser des utilisateurs spécifiques à accéder à l'objet S3 et à le lire. Si votre organisation a été créée en utilisant AWS Organizations, vous devez faire en sorte que personne ne puisse modifier les balises ajoutées par GuardDuty.

Pour plus d'informations, consultez [la section Empêcher la modification des balises, sauf par des personnes autorisées](#), dans le Guide de l'AWS Organizations utilisateur. L'exemple utilisé dans le sujet lié mentionne `ec2`. Lorsque vous utilisez cet exemple, remplacez `ec2` par `s3`.

La liste suivante explique ce que vous pouvez faire à l'aide du TBAC :

- Empêchez tous les utilisateurs, à l'exception du principal de service Malware Protection for S3, de lire les objets S3 qui ne sont pas encore balisés avec la paire clé-valeur de balise suivante :

GuardDutyMalwareScanStatus:*Potential key value*

- GuardDuty Autoriser uniquement l'ajout de la clé de balise GuardDutyMalwareScanStatus avec une valeur comme résultat de numérisation, à un objet S3 scanné. Le modèle de politique suivant peut permettre à des utilisateurs spécifiques ayant accès de potentiellement remplacer la paire clé-valeur du tag.

Exemple de politique de ressources du compartiment S3 :

Remplacez les valeurs d'espace réservé suivantes dans l'exemple de politique :

- *IAM-role-name*- Indiquez le rôle IAM que vous avez utilisé pour configurer Malware Protection pour S3 dans votre compartiment.

- **555555555555**- Fournissez le compartiment Compte AWS associé au compartiment protégé.
- **amzn-s3-demo-bucket**- Indiquez le nom du compartiment protégé.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "NoReadUnlessClean",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
        "arn:aws:iam::555555555555:role/IAM-role-name"
      ]
    },
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringNotEquals": {
        "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
        "NO_THREATS_FOUND"
      }
    }
  },
  {
    "Sid": "OnlyGuardDutyCanTagScanStatus",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
        "arn:aws:iam::555555555555:role/IAM-role-name"
      ]
    },
    "Action": "s3:PutObjectTagging",
    "Resource": "arn:aws:s3::amzn-s3-demo-bucket/*",
    "Condition": {
```

```
    "ForAnyValue:StringEquals": {  
      "s3:RequestObjectTagKeys": "GuardDutyMalwareScanStatus"  
    }  
  }  
}
```

Pour plus d'informations sur le balisage de votre ressource S3, les politiques de [balisage et de contrôle d'accès](#).

Affichage et compréhension de l'état du compartiment protégé

Après avoir activé Malware Protection for S3 pour un compartiment, l'état indique si la fonctionnalité est configurée et fonctionne comme prévu. Ce statut est associé à un identifiant (ID) unique du plan de protection contre les logiciels malveillants. GuardDuty crée cet identifiant au moment de l'activation de la fonctionnalité.

Pour consulter le statut de votre bucket protégé, procédez comme suit :

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Malware Protection for S3.
3. Dans le tableau des compartiments protégés, consultez la colonne État correspondante pour votre compartiment S3.

Le tableau suivant répertorie et décrit les valeurs d'état associées à la ressource de votre plan de protection contre les programmes malveillants. En comprenant ce que ces statuts signifient pour votre compartiment protégé, vous pouvez mieux vous assurer qu'il GuardDuty lance une analyse automatique des programmes malveillants lorsqu'un objet est chargé.

Statut	Description
Actif	<p>Votre compartiment S3 a été correctement configuré avec Malware Protection for S3.</p> <p>Lorsque le statut est Actif, les modifications apportées au rôle IAM (suppression ou modification des autorisations) ne</p>

Statut	Description
	mettent pas le statut Avertissement ou Erreur à jour. Nous vous recommandons de surveiller en permanence l'état du scan en utilisant l'une des méthodes décrites dans Surveillance des scans d'objets S3 .
Avertissement [*] -	La protection contre les programmes malveillants pour S3 est conçue pour ne pas être affectée lorsqu'un avertissement apparaît. Lorsqu' GuardDuty il détecte un nouvel objet S3, il lance une analyse des logiciels malveillants. Une fois l'analyse lancée avec succès, la valeur de la colonne Status peut prendre quelques minutes pour passer à Active. Vous recevrez une EventBridge notification après la mise à jour de la valeur de la colonne État.
Erreur [*] -	Votre seau n'est pas protégé. Aucune des analyses de programmes malveillants associées à ce compartiment S3 ne sera terminée. Il peut y avoir une ou plusieurs causes profondes potentielles.

* Pour plus d'informations sur les problèmes potentiels et les étapes correspondantes pour les résoudre, consultez [Résolution des problèmes liés à l'état du plan de protection](#).

Surveillance des scans d'objets S3 dans Malware Protection for S3

Lorsque vous utilisez Malware Protection for S3 avec un identifiant de GuardDuty détecteur, si votre objet Amazon S3 est potentiellement malveillant, il GuardDuty sera généré [Protection contre les programmes malveillants pour le type de recherche S3](#). À l'aide de la GuardDuty console et des API, vous pouvez consulter les résultats générés. Pour plus d'informations sur la compréhension de ce type de recherche, consultez [Détails d'un résultat](#).

Lorsque vous utilisez Malware Protection for S3 sans l'activer GuardDuty (aucun identifiant de détecteur), même si votre objet Amazon S3 scanné est potentiellement malveillant, GuardDuty vous ne pouvez générer aucun résultat.

Table des matières

- [État du scan potentiel de l'objet S3 et état des résultats](#)
- [Surveillance des scans d'objets S3 avec Amazon EventBridge](#)
- [Surveillance des scans d'objets S3 à l'aide de balises GuardDuty gérées](#)
- [Métriques d'état d'analyse des objets S3 dans CloudWatch](#)

État du scan potentiel de l'objet S3 et état des résultats

Cette section explique les valeurs d'état d'analyse potentielles des objets S3 et les valeurs des résultats d'analyse.

L'état d'analyse d'un objet S3 indique l'état de l'analyse des programmes malveillants, par exemple terminée, ignorée ou échouée.

L'état du résultat de l'analyse des programmes malveillants d'un objet S3 indique le résultat de l'analyse en fonction de la valeur de l'état d'analyse. La valeur d'état de chaque résultat d'analyse de programmes malveillants correspond à un état d'analyse.

La liste suivante fournit les valeurs potentielles des résultats d'analyse des objets S3. Si vous avez activé le balisage, vous pouvez surveiller le résultat de l'analyse en [Utilisation des balises d'objets S3](#). Après l'analyse, la valeur de la balise aura l'une des valeurs de résultat d'analyse suivantes.

Valeurs d'état des résultats d'analyse des malwares potentiels d'un objet S3

- NO_THREATS_FOUND— n'a GuardDuty détecté aucune menace potentielle associée à l'objet scanné.
- THREATS_FOUND— GuardDuty a détecté une menace potentielle associée à l'objet scanné.
- UNSUPPORTED— Il existe plusieurs raisons pour lesquelles Malware Protection for S3 ignore une analyse. Les raisons potentielles incluent un fichier protégé par mot de passe, des archives présentant des taux de compression extrêmement élevés et le support de certaines fonctionnalités d'Amazon S3 peut ne pas être disponible. [Protection contre les programmes malveillants pour les quotas S3](#) Pour de plus amples informations, veuillez consulter [Fonctionnalités de protection contre les malwares pour S3](#).
- ACCESS_DENIED— GuardDuty Impossible d'accéder à cet objet pour le scanner. Vérifiez les autorisations de rôle IAM associées à ce compartiment. Pour de plus amples informations, veuillez consulter [Création ou mise à jour d'une politique de rôle IAM](#).

Si vous avez activé le balisage des objets S3 après le scan, consultez. [Résolution des défaillances des balises après numérisation des objets S3](#)

- **FAILED**— GuardDuty impossible d'effectuer une analyse des programmes malveillants sur cet objet en raison d'une erreur interne.

La liste suivante fournit les valeurs d'état potentielles de l'analyse des objets S3 et leur mappage avec le résultat de l'analyse des objets S3.

Valeurs d'état de scan potentiel de l'objet S3

- **Terminé** — L'analyse s'est terminée avec succès et indique si l'objet S3 contient un logiciel malveillant. Dans ce cas, la valeur potentielle du résultat de l'analyse d'un objet S3 peut être l'une **THREATS_FOUND** ou l'autre **NO_THREATS_FOUND**.
- **Ignoré** : GuardDuty ignore une analyse des programmes malveillants lorsque le scan de cet objet S3 n'est pas pris en charge par Malware Protection for S3 ou GuardDuty s'il n'a pas accès à l'objet S3 chargé dans le compartiment sélectionné.

Dans ce cas, la valeur potentielle du résultat de l'analyse d'un objet S3 peut être l'une **UNSUPPORTED** ou l'autre **ACCESS_DENIED**.

GuardDuty ignorera également l'analyse si le rôle IAM requis est supprimé.

- **Échec** : similaire à la valeur du résultat de l'analyse de l'objet S3 **FAILED**, cet état d'analyse signifie qu'il n'a pas été possible d'effectuer une analyse des programmes malveillants sur l'objet S3 en raison d'une erreur interne.

Lorsque l'état du scan est défini **SKIPPED**, la EventBridge notification concernant le résultat de l'analyse de l'objet S3 inclut un **statusReasons** champ à l'intérieur **scanResultDetails**. Ce champ est une liste de chaînes indiquant la raison précise pour laquelle l'analyse a été ignorée. Le tableau suivant décrit les **statusReasons** valeurs possibles.

Motif du statut	État des résultats du scan	Description
UNAUTHORIZED_TO_GET_OBJECT	ACCESS_DENIED	Malware Protection for S3 n'est pas autorisé à lire l'objet S3, ou l'objet S3 n'existe pas. Vérifiez que le rôle IAM associé au compartiment protégé dispose des autorisations requises

Motif du statut	État des résultats du scan	Description
		et que toute AWS KMS politique de compartiment autorise le rôle à déchiffrer des objets.
UNAUTHORIZED_TO_ASSUME_ROLE	ACCESS_DENIED	Malware Protection for S3 ne peut pas assumer le rôle IAM configuré pour le compartiment protégé. Vérifiez que la politique d'approbation des rôles autorise Malware Protection for S3 à assumer le rôle.
SSE_C_ENCRYPTED_OBJECT	ACCESS_DENIED	L'objet S3 est chiffré à l'aide d'une clé de chiffrement fournie par le client (SSE-C). GuardDuty Impossible d'accéder aux objets chiffrés avec SSE-C. Pour de plus amples informations, veuillez consulter Supportabilité des fonctionnalités d'Amazon S3 .
OBJECT_ETAG_CHANGED	ACCESS_DENIED	L'ETag de l'objet S3 a changé entre le moment où l'analyse a été lancée et le moment où l'on GuardDuty a tenté de lire l'objet. Le téléchargement suivant ou la nouvelle version sera scanné.
BUCKET_NOT_FOUND	ACCESS_DENIED	Le compartiment S3 associé à l'analyse n'existe plus.
UNSUPPORTED_STORAGE_CLASS	UNSUPPORTED	L'objet S3 utilise une classe de stockage qui n'est pas prise en charge par Malware Protection for S3. Pour de plus amples informations, veuillez consulter Supportabilité des fonctionnalités d'Amazon S3 .

Motif du statut	État des résultats du scan	Description
OBJECT_SIZE_LIMIT_EXCEEDED	UNSUPPORTED	La taille de l'objet S3 dépasse la limite de taille de fichier maximale pour Malware Protection for S3. Pour de plus amples informations, veuillez consulter Protection contre les programmes malveillants pour les quotas S3 .
PASSWORD_PROTECTED	UNSUPPORTED	L'objet est protégé par mot de passe.
EXTRACTED_FILE_LIMIT_EXCEEDED	UNSUPPORTED	L'archive contient un nombre de fichiers supérieur à la limite maximale autorisée. Pour de plus amples informations, veuillez consulter Protection contre les programmes malveillants pour les quotas S3 .
EXTRACTED_LEVEL_LIMIT_EXCEEDED	UNSUPPORTED	L'archive dépasse la profondeur d'imbrication maximale autorisée.
EXTRACTED_BYTE_LIMIT_EXCEEDED	UNSUPPORTED	Le contenu de l'archive extrait dépasse la taille maximale autorisée en octets. Pour de plus amples informations, veuillez consulter Protection contre les programmes malveillants pour les quotas S3 .
EXTRACTION_RATIO_LIMIT_EXCEEDED	UNSUPPORTED	L'archive présente un taux de compression extrêmement élevé qui dépasse la limite autorisée. Pour de plus amples informations, veuillez consulter Protection contre les programmes malveillants pour les quotas S3 .

Surveillance des scans d'objets S3 avec Amazon EventBridge

Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications Software-as-a-Service (SaaS) et AWS services et achemine ces données vers des cibles telles que Lambda. Cela vous permet de surveiller les événements qui se produisent dans les services et de créer des architectures basées sur les événements. Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

En tant que compte propriétaire d'un compartiment S3 protégé par Malware Protection for S3, il GuardDuty publie EventBridge des notifications sur le bus d'événements par défaut dans les scénarios suivants :

- La protection contre les programmes malveillants planifie les modifications de l'état des ressources pour tous vos compartiments protégés. Pour plus d'informations sur les différents statuts, consultez [Affichage et compréhension de l'état du compartiment protégé](#).

Pour configurer la règle Amazon EventBridge (EventBridge) pour le statut des ressources, consultez [État des ressources du plan de protection contre les logiciels malveillants](#).

- Le résultat de l'analyse des objets S3 est publié sur votre bus d' EventBridge événements par défaut.

Le `s3Throttled` champ indique s'il y a eu un retard dans le chargement ou la récupération du stockage depuis Amazon S3. La valeur `true` indique qu'il y a eu un retard et `false` qu'il n'y a pas eu de retard.

Si `s3Throttled` c'est `true` pour le résultat de votre analyse, Amazon S3 recommande de configurer des préfixes de manière à réduire le nombre de transactions par seconde (TPS) pour chaque préfixe. Pour plus d'informations, consultez la section [Modèles de conception des meilleures pratiques : optimisation des performances d'Amazon S3](#) dans le guide de l'utilisateur Amazon S3.

Pour configurer la règle Amazon EventBridge (EventBridge) pour les résultats d'analyse des objets S3, consultez [Résultat de l'analyse d'objets S3](#).

- Il y a un événement d'échec de la balise après le scan pour les raisons suivantes :
 - Votre rôle IAM ne dispose pas des autorisations nécessaires pour étiqueter l'objet.

Le [Ajouter des autorisations de politique IAM](#) modèle inclut l'autorisation de GuardDuty baliser un objet.

- La ressource ou l'objet du bucket spécifié dans le rôle IAM n'existe plus.
- L'objet S3 associé a déjà atteint la limite maximale de balises. Pour plus d'informations sur la limite de balises, consultez la section [Catégorisation de votre stockage à l'aide de balises](#) dans le guide de l'utilisateur Amazon S3.

Pour configurer la règle Amazon EventBridge (EventBridge) pour les événements de défaillance des balises après le scan, consultez [Post-scan événements de défaillance des balises](#).

Configurer des EventBridge règles

Vous pouvez configurer des EventBridge règles dans votre compte pour envoyer soit l'état des ressources, soit les événements d'échec des balises après le scan, soit le résultat de l'analyse des objets S3 à une autre Service AWS personne. En tant que compte GuardDuty administrateur délégué, vous recevrez la notification de l'état des ressources du plan de protection contre les programmes malveillants en cas de modification du statut.

La EventBridge tarification standard s'appliquera. Pour plus d'informations, consultez les [EventBridge tarifs Amazon](#).

Toutes les valeurs qui apparaissent dans *red* sont des espaces réservés pour l'exemple. Ces valeurs changeront en fonction des valeurs de votre compte et de la détection ou non d'un logiciel malveillant.

Rubriques

- [État des ressources du plan de protection contre les logiciels malveillants](#)
- [Résultat de l'analyse d'objets S3](#)
- [Post-scan événements de défaillance des balises](#)

État des ressources du plan de protection contre les logiciels malveillants

Vous pouvez créer un modèle d' EventBridge événement basé sur les scénarios suivants :

Valeurs de type de **détail** potentielles

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"

- "GuardDuty Malware Protection Resource Status Error"

Schéma d'événement

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guardduty"]
}
```

Exemple de schéma de notification pour **GuardDuty Malware Protection Resource Status Active** :

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status Active",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ACTIVE"
  }
}
```

Exemple de schéma de notification pour **GuardDuty Malware Protection Resource Status Warning** :

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status warning",
  "source": "aws.guardduty",
  "account": "111122223333",

```

```

    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
      "schemaVersion": "1.0",
      "eventTime": "2024-02-28T01:01:01Z",
      "s3BucketDetails": {
        "bucketName": "amzn-s3-demo-bucket"
      },
      "resourceStatus": "WARNING",
      "statusReasons": [
        {
          "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
        }
      ]
    }
  }
}

```

Exemple de schéma de notification pour **GuardDuty Malware Protection Resource Status Error** :

```

{
  "version": "0",
  "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
  "detail-type": "GuardDuty Malware Protection Resource Status Error",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ERROR",
    "statusReasons": [
      {
        "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
      }
    ]
  }
}

```

```
    ]
  }
}
```

En fonction de la raison `resourceStatusERROR`, la `statusReasons` valeur sera renseignée.

Pour plus d'informations sur les étapes de résolution des problèmes liés aux avertissements et erreurs suivants, consultez [Résolution des problèmes liés à l'état du plan de protection](#).

Résultat de l'analyse d'objets S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Lorsque `scanStatus` c'est le cas `SKIPPED`, il `scanResultDetails` inclut un `statusReasons` champ qui fournit la raison précise pour laquelle le scan a été ignoré. Pour plus d'informations sur les valeurs possibles, consultez [État du scan potentiel de l'objet S3 et état des résultats](#).

Exemple de schéma de notification pour **NO_THREATS_FOUND** :

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    }
  }
}
```

```

    },
    "scanResultDetails": {
      "scanResultStatus": "NO_THREATS_FOUND",
      "threats": null,
      "statusReasons": null
    }
  }
}

```

Exemple de schéma de notification pour **THREATS_FOUND** :

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "THREATS_FOUND",
      "threats": [
        {
          "name": "EICAR-Test-File (not a virus)",
          "source": "AMAZON",
          "itemDetails": [{
            "hash":
              "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855",
            "itemPath": "APKAEIBAERJR2EXAMPLE"
          }]
        }
      ]
    }
  }
}

```



```

    }
  ],
  "statusReasons": null
}
}
}

```

Note

Le `scanResultDetails.Threats` champ ne contient qu'une seule menace. Par défaut, le scan Malware Protection for S3 signale la première menace détectée. Ensuite, le `scanStatus` est réglé sur `COMPLETED`.

Exemple de schéma de notification pour l'état des résultats du scan **UNSUPPORTED** (ignoré) :

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "UNSUPPORTED",
      "threats": null,
      "statusReasons": ["PASSWORD_PROTECTED"]
    }
  }
}

```

```
}
}
```

Exemple de schéma de notification pour l'état des résultats du scan **ACCESS_DENIED** (ignoré) :

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "ACCESS_DENIED",
      "threats": null,
      "statusReasons": ["SSE_C_ENCRYPTED_OBJECT"]
    }
  }
}
```

Exemple de schéma de notification pour l'état des résultats du scan **FAILED** :

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
```

```

    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
      "schemaVersion": "1.0",
      "scanStatus": "FAILED",
      "resourceType": "S3_OBJECT",
      "s3ObjectDetails": {
        "bucketName": "amzn-s3-demo-bucket",
        "objectKey": "APKAEIBAERJR2EXAMPLE",
        "eTag": "ASIAI44QH8DHBEXAMPLE",
        "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
        "s3Throttled": false
      },
      "scanResultDetails": {
        "scanResultStatus": "FAILED",
        "threats": null,
        "statusReasons": null
      }
    }
  }
}

```

Post-scan événements de défaillance des balises

Schéma de l'événement :

```

{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty"
}

```

Exemple de schéma de notification pour **ACCESS_DENIED** :

```

{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],

```

```

    "detail": {
      "schemaVersion": "1.0",
      "eventTime": "2024-06-10T16:16:08Z",
      "s3ObjectDetails": {
        "bucketName": "amzn-s3-demo-bucket",
        "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
        "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
        "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
        "s3Throttled": false
      },
      "postScanActions": [{
        "actionType": "TAGGING",
        "failureReason": "ACCESS_DENIED"
      }]
    }
  }
}

```

Exemple de schéma de notification pour **MAX_TAG_LIMIT_EXCEEDED** :

```

{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
      "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "postScanActions": [{
      "actionType": "TAGGING",
      "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
    }]
  }
}

```

```
}  
}
```

Pour résoudre ces causes de défaillance, voir [Résolution des défaillances des balises après numérisation des objets S3](#).

Surveillance des scans d'objets S3 à l'aide de balises GuardDuty gérées

Utilisez l'option d'activation du balisage afin d'ajouter des balises à votre objet Amazon S3 une fois l'analyse des logiciels malveillants terminée.

Considérations relatives à l'activation du balisage

- Il y a un coût d'utilisation associé lorsque vous GuardDuty balisez vos objets S3. Pour de plus amples informations, veuillez consulter [Tarification et coût d'utilisation de Malware Protection for S3](#).
- Vous devez conserver les autorisations de balisage requises pour votre rôle IAM préféré associé à ce compartiment ; sinon, GuardDuty vous ne pourrez pas ajouter de balises à vos objets numérisés. Le rôle IAM inclut déjà les autorisations permettant d'ajouter des balises aux objets S3 scannés. Pour de plus amples informations, veuillez consulter [Création ou mise à jour d'une politique de rôle IAM](#).
- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet S3. Pour de plus amples informations, veuillez consulter [Utilisation du contrôle d'accès basé sur des balises \(TBAC\)](#).

Une fois que vous avez activé le balisage pour un compartiment S3 ou pour des préfixes spécifiques, tout objet récemment chargé qui est scanné sera associé à une balise au format de paire clé-valeur suivant :

GuardDutyMalwareScanStatus:*Scan-Result-Status*

Pour plus d'informations sur les valeurs de balise potentielles, consultez [État du scan potentiel de l'objet S3 et état des résultats](#).

Résolution des défaillances des balises après le scan des objets S3 dans Malware Protection for S3

Cette section ne s'applique à vous que si vous êtes [Activer le balisage pour les objets numérisés](#) dans votre compartiment protégé.

Lorsque GuardDuty vous tentez d'ajouter une balise à votre objet S3 scanné, l'action de balisage peut entraîner un échec. Les raisons potentielles pour lesquelles cela peut arriver à votre compartiment sont ACCESS_DENIED et MAX_TAG_LIMIT_EXCEEDED. Consultez les rubriques suivantes pour comprendre les causes potentielles de ces défaillances des balises après le scan et pour les résoudre.

ACCÈS REFUSÉ

La liste suivante fournit les raisons potentielles pouvant être à l'origine de ce problème :

- L'AllowPostScanTagautorisation n'est pas requise pour le rôle IAM utilisé pour ce compartiment S3 protégé. Vérifiez que le rôle IAM associé utilise cette politique de compartiment. Pour de plus amples informations, veuillez consulter [Création ou mise à jour d'une politique de rôle IAM](#).
- La politique de compartiment S3 protégé n'autorise pas GuardDuty l'ajout de balises à cet objet.
- L'objet S3 scanné n'existe plus.

MAX_TAG_LIMIT_EXCEEDED

Par défaut, vous pouvez associer jusqu'à 10 balises à un objet S3. Pour plus d'informations, consultez la section Considérations relatives GuardDuty à l'ajout d'une balise à votre objet S3 sous [Activer le balisage pour les objets numérisés](#).

Métriques d'état d'analyse des objets S3 dans CloudWatch

Vous pouvez surveiller GuardDuty l'utilisation CloudWatch, qui collecte les données brutes et les transforme en indicateurs lisibles en temps quasi réel. Ces statistiques sont conservées pendant 15 mois, afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de Malware Protection for S3. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Les CloudWatch métriques relatives à Malware Protection for S3 sont disponibles au niveau des ressources. Vous pouvez interroger ces métriques séparément pour chaque ressource protégée. Les métriques sont signalées dans l'espace de AWS/GuardDuty/MalwareProtection noms. Vous pouvez configurer des alarmes sur des ressources spécifiques afin de surveiller le niveau de sécurité.

Mesures d'état de l'analyse des programmes malveillants

Métrique	Description
----------	-------------

CompletedScanCount

Nombre d'analyses de programmes malveillants sur des objets S3 effectuées dans un laps de temps donné.

Dimensions valides :

- Malware Protection Plan Id

Resource Name

Unités : nombre

FailedScanCount

Nombre d'analyses de programmes malveillants sur des objets S3 qui ont échoué au cours d'une période donnée.

Dimensions valides :

- Malware Protection Plan Id

Resource Name

Unités : nombre

SkippedScanCount

Nombre d'analyses de programmes malveillants sur des objets S3 qui ont été ignorées au cours d'une période donnée.

Dimensions valides :

- Malware Protection Plan Id

Resource Name

Skipped Reason

Valeurs potentielles

- Unsupported
- MissingPermissions

Unités : nombre

Mesures des résultats de l'analyse des logiciels malveillants

InfectedScanCount

Nombre d'analyses de programmes malveillants sur des objets S3 qui ont détecté un objet potentiellement malveillant au cours d'une période donnée.

Dimensions valides :

- Malware Protection Plan Id

Resource Name

Unités : nombre

CompletedScanBytes

Le nombre d'octets d'objets S3 analysés au cours d'une période donnée.

Dimensions valides :

- Malware Protection Plan Id

Resource Name

Unités : nombre

Note

Par défaut, les statistiques des CloudWatch métriques sont AVG.

Les dimensions suivantes sont prises en charge pour les métriques de protection contre les programmes malveillants pour S3.

Dimension	Description
Malware Protection Plan Id	Identifiant unique associé à la ressource du plan de protection contre les programmes malveillants GuardDuty créée pour votre ressource protégée.
Resource Name	Le nom de la ressource protégée.
Skipped Reason	La raison pour laquelle une analyse des malwares liés à un objet S3 a été ignorée.
Valeurs potentielles	
<ul style="list-style-type: none">• Unsupported• MissingPermissions	

Pour plus d'informations sur l'accès à ces statistiques et leur interrogation, consultez la section [Utiliser CloudWatch les métriques Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations sur la configuration des alarmes, consultez la section [Utilisation des CloudWatch alarmes Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Résolution des problèmes

Table des matières

- [Résolution des problèmes liés à l'état du plan de protection](#)
- [Résolution des problèmes liés au scan des programmes malveillants](#)

Résolution des problèmes liés à l'état du plan de protection

Pour tout compartiment protégé, GuardDuty affiche le statut en fonction du classement. Par exemple, si un bucket protégé présente des problèmes dans les catégories Erreur et Avertissement, GuardDuty il affichera d'abord le problème associé au statut d'erreur.

La liste suivante inclut les erreurs et l'avertissement concernant l'état du plan de protection contre les programmes malveillants.

Erreurs

- [EventBridge la notification est désactivée pour ce compartiment S3](#)
- [EventBridge la règle gérée pour recevoir les événements du compartiment S3 est manquante](#)
- [Le compartiment S3 n'existe plus](#)

Warning (Avertissement)

[Impossible de mettre l'objet de test](#)

EventBridge la notification est désactivée pour ce compartiment S3

Le code de motif du statut associé est `EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Détail du statut

GuardDuty utilise EventBridge pour recevoir une notification lorsqu'un nouvel objet est chargé dans ce compartiment S3. Cette autorisation est absente de votre rôle IAM.

Étapes de résolution des problèmes

Option 1 : ajoutez la déclaration d'autorisation suivante à votre rôle IAM :

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
}
```

amzn-s3-demo-bucket Remplacez-le par le nom de votre compartiment Amazon S3.

Option 2 : activer les EventBridge notifications à l'aide de la console Amazon S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Sur la page Compartiments, sous l'onglet Compartiments à usage général, sélectionnez le nom du compartiment associé à cette erreur.
3. Sur cette page de bucket, choisissez l'onglet Propriétés.
4. Dans la EventBridge section Amazon, sélectionnez Modifier.
5. Sur la EventBridge page Modifier Amazon, pour Envoyer une notification à Amazon EventBridge pour tous les événements de ce compartiment, sélectionnez Activé.
6. Sélectionnez Enregistrer les modifications.

Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

EventBridge la règle gérée pour recevoir les événements du compartiment S3 est manquante

Le code de motif du statut associé est `EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Détail du statut

Les autorisations des règles EventBridge gérées permettant de gérer la configuration des EventBridge règles sont manquantes.

Étapes de résolution des problèmes

Ajoutez la déclaration d'autorisation suivante à votre rôle IAM :

```
{
  "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
  "Effect": "Allow",
  "Action": [
    "events:PutRule",
    "events>DeleteRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource": [
    "arn:aws:events::*:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
  ],
  "Condition": {
    "StringEquals": {
      "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
    }
  }
}
```

Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

Le compartiment S3 n'existe plus

Le code de motif du statut associé est `PROTECTED_RESOURCE_DELETED`.

Détail du statut

Ce compartiment S3 a été supprimé de votre compte et n'existe plus.

Étape de résolution des problèmes

Si la suppression du compartiment S3 n'était pas intentionnelle, vous pouvez en créer un nouveau à l'aide de la console Amazon S3.

Une fois le compartiment créé avec succès, activez Malware Protection for S3 en suivant les étapes décrites dans la [Configuration de la protection contre les programmes malveillants pour S3 pour votre bucket](#) page.

Impossible de mettre l'objet de test

Le code de motif du statut associé est `INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

Note

L'autorisation d'ajouter un objet de test est facultative. L'absence de cette autorisation dans votre rôle IAM n'empêche pas Malware Protection for S3 de lancer une analyse des programmes malveillants sur un objet récemment chargé. Une fois l'analyse lancée avec succès, le passage de l'état du plan de protection contre les programmes malveillants de Avertissement à Actif peut prendre quelques minutes.

Si le rôle IAM inclut déjà cette autorisation, cet avertissement indique une politique de compartiment Amazon S3 restrictive qui n'autorise pas l'accès IAM pour placer l'objet de test dans ce compartiment S3.

Détail du statut

Pour valider la configuration du bucket sélectionné, GuardDuty place un objet de test dans votre bucket.

Étapes de résolution des problèmes

Vous pouvez choisir de mettre à jour le rôle IAM pour inclure les autorisations manquantes. Au rôle IAM sélectionné, ajoutez les autorisations suivantes GuardDuty afin de placer l'objet de test sur la ressource sélectionnée :

```
{
    "Sid": "AllowPutValidationObject",
    "Effect": "Allow",
```

```
"Action": [  
    "s3:PutObject"  
  ],  
  "Resource": [  
    "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"  
  ]  
}
```

amzn-s3-demo-bucket Remplacez-le par le nom de votre compartiment Amazon S3. Pour plus d'informations sur les autorisations des rôles IAM, consultez [Création ou mise à jour d'une politique de rôle IAM](#).

Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

Résolution des problèmes liés au scan des programmes malveillants

Impossible de démarrer un scan.

Assurez-vous que la demande d'analyse contient des données valides et que le plan de protection contre les programmes malveillants est activé pour le compartiment.

Modification du plan de protection contre les programmes malveillants pour un compartiment protégé

Vous devrez peut-être modifier la politique d'autorisation IAM préférée, activer ou désactiver le balisage de l'objet S3 scanné, ou ajouter ou supprimer des préfixes d'objet S3. Par exemple, lorsque vous avez activé Malware Protection for S3 pour votre compartiment, vous avez décidé de ne pas activer le balisage de l'objet S3 scanné avec le résultat de l'analyse. Cependant, vous souhaitez maintenant GuardDuty ajouter la balise prédéfinie et le résultat de l'analyse en tant que valeur de balise.

Choisissez une méthode d'accès préférée pour mettre à jour le plan de protection contre les programmes malveillants de votre compartiment S3 protégé.

Console

Pour modifier un plan de protection contre les programmes malveillants

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Malware Protection for S3.
3. Sous Compartiments protégés, sélectionnez le compartiment pour lequel vous souhaitez modifier la configuration existante.
4. Choisissez Modifier.
5. Mettez à jour la configuration et les paramètres existants de votre compartiment et confirmez les modifications. Pour plus d'informations sur la description et les étapes de chaque section, consultez [Activation de la protection contre les programmes malveillants pour S3 pour votre bucket](#).

Surveillez la colonne État de ce compartiment protégé. S'il apparaît sous la forme d'un avertissement ou d'une erreur, consultez [Résolution des problèmes liés à l'état du plan de protection](#).

API/CLI

Pour modifier le plan de protection contre les programmes malveillants à l'aide de l'API ou AWS CLI

- En utilisant l'API

Exécutez l'[UpdateMalwareProtectionPlan](#) API en utilisant l'ID du plan de protection contre les logiciels malveillants associé à cette ressource de plan.

Pour récupérer l'ID du plan de protection contre les programmes malveillants dans une région spécifique, vous pouvez exécuter l'[ListMalwareProtectionPlans](#) API dans cette région.

- En utilisant AWS CLI

La liste suivante fournit des AWS CLI exemples de commandes pour mettre à jour la ressource du plan de protection contre les programmes malveillants. Vous aurez besoin de l'ID du plan de protection contre les programmes malveillants associé à votre compartiment S3.

AWS CLI exemples de commandes

- Utilisez la AWS CLI commande suivante pour activer ou désactiver le balisage pour la ressource du plan de protection contre les programmes malveillants associée à votre compartiment S3 :

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
```

- Utilisez la AWS CLI commande suivante pour ajouter un préfixe d'objet à la ressource du plan de protection contre les programmes malveillants associée à votre compartiment S3 :

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
```

Assurez-vous d'inclure les préfixes d'objets existants dans cette commande ; sinon, ces préfixes GuardDuty seront supprimés lors de la modification de la ressource du plan de protection contre les programmes malveillants.

- Utilisez la AWS CLI commande suivante pour supprimer un préfixe d'objet de la ressource du plan de protection contre les programmes malveillants associée à votre compartiment S3 :

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
```

Si vous ne possédez pas encore l'ID du plan de protection contre les programmes malveillants pour cette ressource, vous pouvez exécuter la AWS CLI commande suivante et la *us-east-1* remplacer par la région pour laquelle vous souhaitez répertorier les identifiants du plan de protection contre les programmes malveillants.

```
aws guardduty list-malware-protection-plans --region us-east-1
```


Désactivation de la protection contre les programmes malveillants pour S3 pour un compartiment protégé

Lorsque vous désactivez la protection contre les programmes malveillants pour S3 pour un compartiment protégé, l'ID du GuardDuty plan de protection contre les programmes malveillants associé à ce compartiment est supprimé. GuardDuty ne lancera plus d'analyse des programmes malveillants lorsqu'un nouvel objet est chargé dans ce compartiment ou dans l'un des préfixes d'objets sélectionnés.

Si vous avez activé GuardDuty et souhaitez maintenant le suspendre ou le désactiver GuardDuty, consultez [Suspension ou désactivation GuardDuty](#). Comme il n'existe aucun concept d'identifiant de détecteur dans Malware Protection for S3, la désactivation ou la suspension GuardDuty n'a aucune incidence sur le statut d'un compartiment protégé dans votre compte. Vous pouvez continuer à utiliser la fonctionnalité Malware Protection for S3 indépendamment avec le tarif standard associé. Pour de plus amples informations, veuillez consulter [Révision du coût d'utilisation de Malware Protection for S3](#). Pour arrêter d'utiliser Malware Protection for S3, vous devez la désactiver pour tous les compartiments protégés de votre compte. Si vous souhaitez continuer à utiliser GuardDuty et désactiver uniquement Malware Protection for S3 pour un bucket, les étapes suivantes n'auront aucune incidence sur la configuration du GuardDuty service ni sur les autres plans de protection que vous avez peut-être activés.

Choisissez une méthode d'accès préférée pour désactiver la protection contre les programmes malveillants pour S3 dans votre compartiment S3 protégé.

Console

Pour désactiver la protection contre les programmes malveillants pour S3 à l'aide de GuardDuty la console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Malware Protection for S3.
3. Sous Compartiments protégés, sélectionnez le compartiment pour lequel vous souhaitez désactiver la protection contre les programmes malveillants pour S3.

Vous ne pouvez sélectionner qu'un seul compartiment protégé à la fois. Pour désactiver la protection contre les programmes malveillants pour S3 pour plusieurs compartiments, suivez à nouveau ces étapes pour un autre compartiment S3.

4. Choisissez Désactiver pour confirmer la sélection.

API/CLI

Pour désactiver la protection contre les programmes malveillants pour S3 à l'aide de l'API ou AWS CLI

- En utilisant l'API

Exécutez l'[DeleteMalwareProtectionPlan](#) API en utilisant l'ID du plan de protection contre les logiciels malveillants associé à cette ressource de plan.

Pour récupérer l'identifiant du plan de protection contre les malwares, vous pouvez exécuter l'[ListMalwareProtectionPlans](#) API.

- En utilisant AWS CLI

Vous pouvez également exécuter la AWS CLI commande suivante pour désactiver la protection contre les programmes malveillants pour S3 en le `4cc8bf26c4d75EXAMPLE` remplaçant par l'ID du plan de protection contre les programmes malveillants associé à ce compartiment S3 :

```
aws guardduty delete-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE
```

Si vous ne possédez pas encore l'ID du plan de protection contre les programmes malveillants pour ce compartiment S3, vous pouvez exécuter la AWS CLI commande suivante et le `us-east-1` remplacer par la région pour laquelle vous souhaitez répertorier les identifiants du plan de protection contre les programmes malveillants.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Supportabilité des fonctionnalités d'Amazon S3

Le tableau suivant indique si Malware Protection for S3 prend en charge les fonctionnalités Amazon S3 répertoriées.

Le support est-il disponible ?	Description
Oui	Les objets S3 peuvent être récupérés sans restauration asynchrone.

Le support est-il disponible ?	Description
Conditionnel	<ul style="list-style-type: none">• La prise en charge de la hiérarchisation intelligente est disponible pour les objets S3 dans les niveaux Frequent, Infrequent et Archive Instance Access.• Les niveaux opt-in Archive et Deep Archive ne sont pas pris en charge.• La hiérarchisation intelligente crée toujours un nouvel objet dans le niveau Accès fréquent. Par conséquent, le scan d'objets lors de la création est pris en charge.• Les futures fonctionnalités de hiérarchisation intelligente pourraient démarrer les objets dans Archive. Par conséquent, cela n'est pas pris en charge.

Le support est-il disponible ?	Description
Non	GuardDuty ne prend en charge que les compartiments à usage général pour la protection contre les logiciels malveillants pour S3.

Le support est-il disponible ?	Description
Non	Les objets S3 doivent être restaurés avant d'être accessibles.
Non	La protection contre les programmes malveillants pour S3 n'est pas prise en charge sur Outposts.

Le support est-il disponible ?	Description
Oui	<p>Tous les objets S3 chargés sont analysés pour détecter la présence de malwares. Si vous avez chargé un objet avec la version de fichier v1 et que vous avez immédiatement téléchargé une autre version, remplacez par v2, les versions v1 et v2 du fichier objet GuardDuty seront analysées à la fois. Cependant, il se peut que l'heure de début de l'analyse ne soit pas dans le même ordre.</p>
Oui	<p>Si le compartiment de destination est une ressource protégée, il GuardDuty analysera tous les objets S3 répliqués vers les préfixes protégés et surveillés.</p>
Non	<p>Vous ne pouvez pas définir de règle de réplication en fonction de la balise de résultat du scan. Amazon S3 ne prend pas en charge la réplication pour les balises, sauf lors de la création.</p>

Le support est-il disponible ?	Description
Oui	<p>GuardDuty prend en charge les analyses de programmes malveillants pour les objets S3 chiffrés à l'aide de clés gérées et gérées par le client. Assurez-vous que le rôle IAM inclut l'autorisation d'utiliser la clé. Pour de plus amples informations, veuillez consulter Ajouter des autorisations de politique IAM.</p>

Le support est-il disponible ?	Description
Non	Malware Protection for S3 ne prend pas en charge l'analyse des objets S3 chiffrés avec des clés inaccessibles.
Non	<p>Lorsque vos objets Amazon S3 sont chiffrés à l'aide du client de chiffrement Amazon S3, ils ne sont exposés à aucun tiers, y compris AWS. Pour savoir pourquoi cela n'est pas pris en charge, consultez la section Protection des données à l'aide du chiffrement côté client.</p> <div data-bbox="690 1213 1510 1812"><p> Note</p><p>CSE-KMS les objets chiffrés sont reçus sous forme de blob chiffré dont le chiffrement ne peut pas être déterminé. Par conséquent, il les GuardDuty traite au fur et à mesure de leur réception et analyse le blob chiffré comme un fichier normal. GuardDuty ne renvoie pas d'état de UNSUPPORTED numérisation pour de tels objets, sauf si l'un des résultats est Quotas de protection contre les programmes malveillants pour S3 dépassé.</p></div>

Le support est-il disponible ?	Description
Oui	Les objets S3 verrouillés sont verrouillés sur la base de WORM - Write Once Read Many. Malware Protection for S3 peut accéder aux objets et les scanner.
Oui	Malware Protection for S3 peut scanner les buckets configurés avec Requester Pays. Le demandeur paiera les appels S3. Pour plus d'informations, consultez Utilisation des compartiments de type Paiement par le demandeur pour les transferts et l'utilisation du stockage dans le Guide de l'utilisateur Amazon S3.
Oui	Vous pouvez définir des politiques de cycle de vie en fonction de la balise de résultat du scan. Supprimez automatiquement les objets malveillants, par exemple. Pour plus d'informations sur la configuration du cycle de vie, consultez Gérer le cycle de vie de votre stockage dans le guide de l'utilisateur Amazon S3.

Le support est-il disponible ?	Description
Oui	Vous pouvez définir des politiques de ressources de compartiment en fonction de votre balise de résultat d'analyse d'objets S3. Par exemple, empêchez l'accès aux objets S3 qui ne sont pas encore scannés ou aux menaces GuardDuty détectées. Pour de plus amples informations, veuillez consulter Utilisation du contrôle d'accès basé sur des balises (TBAC) avec Malware Protection pour S3 .
Non	Malware Protection for S3 analyse uniquement le contenu de l'objet S3.

Quotas de protection contre les programmes malveillants pour S3

Cette section fournit des quotas par défaut, souvent appelés limites. Sauf indication contraire, chaque quota est Region-specific. Pour consulter les quotas par défaut spécifiques à l'utilisation du GuardDuty service de base, consultez [GuardDuty Quotas Amazon](#).

Les tableaux suivants décrivent les multiples quotas qui s'appliqueront à votre Compte AWS.

AWS valeur de quota par défaut	Est-il ajustable ?	Description
100 Go	Non	Taille maximale de l'objet S3 qui GuardDuty tentera de rechercher des programmes malveillants.

AWS valeur de quota par défaut	Est-il ajustable ?	Description

AWS valeur de quota par défaut	Est-il ajustable ?	Description
100 000	Non	<p>Nombre maximum de fichiers GuardDuty pouvant être extraits et analysés dans un objet S3.</p> <div><p> Note</p><p>Les types de fichiers composés sont potentiellement soumis à ces limites. Les types de fichiers incluent, sans toutefois s'y limiter, les messages électroniques codés MIME (Multipurpose Internet Mail Extensions), les fichiers Python compilés (PYC), les fichiers d'aide HTML compilés (CHM), tous les programmes d'installation et les documents OpenDocument Format (ODF).</p></div> <div><p> Note</p><p>Les objets S3 présentant un taux de compression extrêmement élevé entre la taille de l'objet S3 et la taille du contenu extrait peuvent être soumis à des limites même si les fichiers extraits sont inférieurs à ce quota.</p></div>

AWS valeur de quota par défaut	Est-il ajustable ?	Description
100	Non	Niveaux d'imbrication maximaux GuardDuty pouvant être extraits dans un objet S3.
25	Non	Le nombre maximum de compartiments S3 pour lesquels vous pouvez activer la protection contre les programmes malveillants pour S3. Cette limite de quota est par compte dans chaque région.

GuardDuty Protection contre les logiciels malveillants pour AWS Sauvegarde

Rubriques

- [Vue d'ensemble](#)
- [Comment fonctionne Malware Protection for Backup ?](#)
- [GuardDuty Protection contre les logiciels malveillants pour les sauvegardes : autorisations relatives aux rôles IAM](#)
- [\(Facultatif\) Commencez à utiliser Malware Protection for Backup Independently \(console uniquement\)](#)
- [Lancement d'un On-Demand scan de protection contre les logiciels malveillants pour Backup](#)
- [Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour Backup](#)
- [Quotas pour la protection contre les logiciels malveillants lors de la sauvegarde](#)

Vue d'ensemble

Malware Protection for Backup vous aide à détecter la présence potentielle de logiciels malveillants dans vos données de sauvegarde en analysant les ressources AWS protégées par Backup, telles que les instantanés Amazon EBS, les AMI Amazon EC2 et les points de restauration Amazon S3. Lorsque AWS Backup crée ou met à jour une ressource de sauvegarde protégée, elle GuardDuty peut effectuer une analyse des programmes malveillants sur cette sauvegarde afin d'identifier le contenu potentiellement malveillant avant qu'il ne soit restauré dans votre environnement.

Comment utiliser Malware Protection for Backup

Vous pouvez utiliser cette fonctionnalité de deux manières, selon qu'elle GuardDuty est activée ou non dans votre compte :

1. Utilisation de Malware Protection for Backup avec l' GuardDuty option activée

Lorsqu'il GuardDuty est activé dans une région, AWS Backup intègre la protection contre les malwares au flux de travail des GuardDuty résultats. Les résultats de l'analyse des programmes malveillants apparaissent dans GuardDuty les résultats, en plus de ceux d'Amazon EventBridge et d'Amazon CloudWatch.

2. Utilisation de Malware Protection for Backup sans activation GuardDuty

Vous pouvez utiliser Malware Protection for Backup indépendamment, sans activer le GuardDuty service complet. Dans ce mode, les résultats de numérisation restent entièrement disponibles via EventBridge et CloudWatch.

Considérations relatives à l'utilisation indépendante de Malware Protection for Backup

Lorsque vous utilisez la fonctionnalité sans l'activer GuardDuty :

- La configuration du plan de sauvegarde est entièrement gérée dans AWS Backup.

GuardDuty ne fournit pas de contrôles pour sélectionner les plans de sauvegarde, les coffres-forts ou les types de ressources. Toutes les fonctions d'activation, de planification et de configuration des politiques restent dans AWS Backup.

- GuardDuty les résultats ne sont pas générés.

Les résultats nécessitent un identifiant de détecteur, qui n'est créé que lorsqu'il GuardDuty est activé. Lorsque vous utilisez Malware Protection de manière indépendante, les résultats de l'analyse sont présentés exclusivement par le biais d' EventBridge événements et de CloudWatch mesures.

- Vous pouvez toujours lancer des analyses à la demande depuis la GuardDuty console.

Même lorsqu'elle n' GuardDuty est pas activée, la GuardDuty console fournit un flux de travail permettant de lancer une analyse des programmes malveillants à la demande pour les types de ressources de sauvegarde pris en charge. Cela permet aux clients d'utiliser une GuardDuty interface familière sans avoir besoin d'un GuardDuty service complet.

- Non-GuardDuty les clients peuvent accéder aux flux de travail de lancement du scan.

Les points d'entrée des scans à la demande sont accessibles à tous les clients utilisant Malware Protection for Backup, qu'un GuardDuty détecteur existe ou non dans le compte.

- Le comportement du scan et la couverture restent identiques.

Qu'elle GuardDuty soit activée ou non, la fonctionnalité analyse les mêmes types de ressources AWS Backup avec le même moteur de détection de malwares. La seule différence réside dans l'endroit où les résultats sont publiés.

Ce modèle permet aux clients d'adopter l'analyse des programmes malveillants pour les sauvegardes sans avoir besoin des fonctionnalités GuardDuty de détection des menaces plus étendues, tout en proposant un GuardDuty-based flux de travail optionnel pour le lancement et la visualisation des opérations d'analyse.

Comment fonctionne Malware Protection for Backup

Malware Protection for Backup peut analyser les ressources protégées par AWS Backup suivantes :

- Instantanés Amazon EBS
- AMI Amazon EC2
- Points de restauration Amazon S3 et [sauvegardes continues ou restauration ponctuelle \(PITR\) S3](#)
- [Coffres-forts verrouillés \(immuables\) \(points de EBS/EC2 restauration\) à l'aide de AWS Backup Vault Lock dans les régions prises en charge](#)

Numérisation incrémentielle

AWS Backup capture les modifications incrémentielles pour de nombreux types de ressources. GuardDuty est capable de scanner uniquement les blocs ou objets nouveaux ou modifiés lors de la création ou de la mise à jour d'une sauvegarde, ce qui améliore les performances et réduit les frais de numérisation tout en garantissant une couverture complète au fil du temps.

On-demand numérisation

Vous pouvez lancer une analyse sur n'importe quelle ressource de sauvegarde prise en charge à tout moment, directement depuis AWS Backup ou depuis la GuardDuty console. Les cas d'utilisation courants incluent la vérification d'une sauvegarde avant la restauration, la revérification des anciennes données après la publication de nouvelles signatures de menaces ou la réalisation d'analyses de conformité périodiques.

Note

- Malware Protection for Backup ne peut être activée que pour les ressources de sauvegarde d'une même région.

- GuardDuty analyse une copie en lecture seule de la sauvegarde ; il ne modifie pas le contenu de la sauvegarde.
- La numérisation fonctionne aussi bien pour les coffres-forts standard que pour les coffres-forts verrouillés (immuables).

Comment fonctionne Malware Protection for Backup ?

Cette section décrit les composants de Malware Protection for Backup, son fonctionnement et la manière dont vous pouvez consulter l'état et les résultats de l'analyse des programmes malveillants.

Vue d'ensemble

Malware Protection for Backup est une fonctionnalité qui vous aide à détecter la présence de logiciels malveillants sur les instantanés EBS, les images EC2 (AMI) et les points de restauration appartenant aux types de ressources EBS, EC2 et S3. Vous pouvez lancer une analyse des programmes malveillants à la demande via la GuardDuty console ou l'API en transmettant un rôle IAM fournissant les autorisations requises pour l'analyse, ainsi qu'un ou deux ARN de ressources en fonction de la catégorie d'analyse. Deux catégories de numérisation sont possibles : les analyses complètes et les analyses incrémentielles.

Scan complet et scan incrémentiel

Lors d'une analyse complète, l'API accepte un ARN de ressource et analyse tous les fichiers contenus dans cette ressource. Une analyse incrémentielle, quant à elle, prend deux ARN de ressources, appartenant toutes deux à la même ressource, et analyse les fichiers modifiés entre elles. Supposons par exemple que nous prenions un instantané d'un volume EBS. Appelons-le snapshot-1. Si une analyse complète est effectuée sur cet instantané, GuardDuty analyse tous les fichiers qu'il contient. Supposons maintenant que quelques fichiers aient été ajoutés au même volume et qu'un nouvel instantané soit pris. Appelons-le snapshot-2. Étant donné que seuls quelques fichiers ont changé entre le snapshot-1 et le snapshot-2, il est possible de déclencher une analyse incrémentielle avec les ARN des ressources de ces deux instantanés. Dans ce cas, snapshot-2 est appelé **target ressource** et snapshot-1 est appelé **ressource base**. Vous verrez cette terminologie utilisée dans le reste du document. Cette analyse incrémentielle analysera les fichiers modifiés entre snapshot-1 et snapshot-2.

Analyse des logiciels malveillants pour Point-in-Time-Recovery (PITR)

Lorsque cette option est activée depuis AWS Backup, l'analyse des programmes malveillants pour les sauvegardes continues ou PITR s'effectue en fonction de la fréquence configurée dans le plan de sauvegarde. Ceci est orchestré par le service AWS Backup. Par exemple, GuardDuty exécutera le premier scan de t0 à t2, le scan suivant de t2 à t4, le scan suivant de t4 à t6 et ainsi de suite. Chacun de ces scans génère un identifiant de scan qui peut être interrogé à l'aide de l'GetMalwareScanAPI pour obtenir le statut et le résultat du scan pour cette période.

Vous pouvez également scanner l'intégralité de la ressource PITR depuis la GuardDuty console ou en utilisant l' GuardDuty StartMalwareScanAPI à la demande en transmettant un horodatage de fin. Cela permettra de GuardDuty scanner l'intégralité de la ressource depuis le début jusqu'à l'horodatage de fin.

Note

- Vous ne pouvez pas déclencher de scans partiels ou incrémentiels sur le PITR à partir de GuardDuty
- L'horodatage de fin transmis pour une analyse à la demande ne peut pas être antérieur à (heure actuelle : 15 minutes).

Nouvelle analyse des fichiers précédemment infectés dans le cadre d'une analyse incrémentielle

Dans le cadre d'une analyse incrémentielle, il GuardDuty réanalysera également les fichiers précédemment infectés à partir de l'analyse de base pendant 365 jours au maximum.

Exigences relatives à une analyse incrémentielle

Les conditions suivantes doivent être remplies pour GuardDuty effectuer une analyse incrémentielle. Si l'une de ces exigences n'est pas remplie, l'analyse GuardDuty sera ignorée.

- La ressource de base doit être scannée au cours des 365 derniers jours et le résultat de l'analyse doit être dans COMPLETED ouCOMPLETED_WITH_ISSUES.
- La date de création de la ressource de base doit être antérieure à celle de la ressource cible.
- Les ressources de base et cible doivent avoir le même type de chiffrement dans le cas des instantanés.

- Les ressources de base et cibles doivent être issues de la même lignée.
 - Pour un instantané EBS et un point de restauration EBS, cela signifie qu'ils proviennent du même volume ou qu'ils proviennent de copies du même volume, sans aucune modification du type de chiffrement.
 - Pour un point de restauration S3, les ARN des ressources de base et cible doivent être créés à partir du même compartiment S3 sous-jacent.
 - Dans le cas des AMI, des paires d'instantanés sont comparées entre l'AMI de base et l'AMI cible afin d'identifier les instantanés à analyser de manière incrémentielle. Chaque paire d'instantanés doit répondre aux conditions mentionnées ci-dessus. Tout instantané de l'AMI cible auquel aucun instantané correspondant ne correspond dans l'AMI de base sera ignoré.

Re-scanning Ressources de sauvegarde précédemment numérisées

Vous pouvez lancer une nouvelle analyse de programmes malveillants à la demande sur la même ressource 10 minutes après le début de la précédente analyse de programmes malveillants. Si la nouvelle analyse des programmes malveillants est lancée dans les 10 minutes suivant le lancement de la précédente, votre demande entraînera l'erreur suivante et aucun identifiant de scan ne sera généré pour cette demande. Les étapes pour réanalyser l'instance restent les mêmes que pour lancer une analyse des programmes malveillants à la demande pour la première fois.

Rôle IAM requis pour la numérisation

Vous devez transmettre un rôle IAM pour démarrer une analyse complète ou incrémentielle. Ce rôle fournit les autorisations requises pour effectuer les opérations d'analyse. [GuardDuty Protection contre les logiciels malveillants pour les sauvegardes : autorisations relatives aux rôles IAM](#) fournit la liste exacte des autorisations requises, ainsi que la politique de confiance pertinente nécessaire pour effectuer l'analyse.

Examen de l'état et du résultat de l'analyse des ressources

GuardDuty publie l'événement du résultat du scan dans le bus d'événements EventBridge par défaut d'Amazon. GuardDuty utilise la livraison au moins une fois, ce qui signifie que vous pouvez recevoir plusieurs résultats de numérisation pour le même objet. Nous vous recommandons de concevoir vos applications de manière à gérer les résultats dupliqués. Vous n'êtes facturé qu'une seule fois pour chaque objet numérisé.

Pour plus d'informations, consultez [Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour Backup](#).

Révision des résultats générés

L'examen des résultats dépend de l'utilisation ou non de Malware Protection for Backup with GuardDuty. Réfléchissez aux scénarios suivants :

Utilisation de Malware Protection for Backup lorsque le GuardDuty service est activé (identifiant du détecteur)

Si l'analyse des programmes malveillants détecte un fichier potentiellement malveillant dans une ressource de sauvegarde scannée, elle GuardDuty générera un résultat associé. Vous pouvez consulter les détails de la recherche et suivre les étapes recommandées pour éventuellement y remédier. En fonction de la [fréquence de vos résultats d'exportation](#), les résultats générés sont exportés vers un compartiment S3 et un bus EventBridge d'événements Amazon.

Pour plus d'informations sur le type de recherche qui serait généré, consultez la section [Protection contre les programmes malveillants pour les types de recherche de Backup](#) Recherche de types pour Malware Protection for Backup.

Utilisation de Malware Protection for Backup en tant que fonctionnalité indépendante (aucun identifiant de détecteur)

GuardDuty ne sera pas en mesure de générer des résultats car aucun identifiant de détecteur n'est associé. Pour connaître l'état du scan de votre ressource de sauvegarde, vous pouvez consulter le résultat du scan qui est GuardDuty automatiquement publié sur votre bus d'événements par défaut.

Pour plus d'informations sur l'état et le résultat de l'analyse, consultez [Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour Backup](#).

Note

Si vous utilisez également Malware Protection pour S3, il est possible que votre fichier S3 ait été précédemment étiqueté comme NO_THREATS_FOUND et que le même fichier apparaisse dans la liste des menaces pour le Backup Recovery Point auquel appartient cet objet. Cela se produit car le service met fréquemment à jour ses signatures de logiciels malveillants, ce qui peut avoir modifié l'état du fichier. Notez que dans de tels cas, il GuardDuty ne sera pas possible de revenir en arrière et de mettre à jour la balise du fichier dans le compartiment S3 d'origine. Le seul moyen d'appliquer une balise mise à jour au fichier est de télécharger à nouveau l'objet dans le compartiment ou d'utiliser la fonction d'analyse à la demande pour S3.

GuardDuty Protection contre les logiciels malveillants pour les sauvegardes : autorisations relatives aux rôles IAM

Rôle du client fourni pour l'analyse des programmes malveillants

GuardDuty Malware Protection s'attend à ce qu'un rôle client (rôle de scanner) soit fourni lorsque des analyses sont lancées sur les ressources de sauvegarde, à savoir les instantanés, les AMI et les points de EBS/EC2/S3 restauration. Ce rôle fournit les autorisations requises GuardDuty pour effectuer l'analyse de ces ressources spécifiques. La politique d'autorisation et la politique de confiance relatives à ce rôle se trouvent dans [Autorisations et politique de confiance pour le rôle](#). La section ci-dessous explique pourquoi chacune de ces autorisations est requise.

Informations sur les autorisations

- **ModifySnapshotAttribute**- Permet d'accéder aux instantanés chiffrés par clé non chiffrés et gérés par le client par le compte du service GuardDuty Malware Protection.
- **CreateGrant**- Permet à GuardDuty Malware Protection de créer et d'accéder à un volume EBS chiffré par clé gérée par le client à partir de l'instantané chiffré par clé gérée par le client auquel le compte de GuardDuty service a accès.
- **RetireGrant**- Permet à GuardDuty Malware Protection de retirer les autorisations créées sur la clé gérée par le client pour lire des instantanés chiffrés
- **ReEncryptTo** et **ReEncryptFrom** - Requis par EBS pour donner GuardDuty accès aux instantanés chiffrés à l'aide de clés gérées par le client et pour créer des volumes chiffrés à partir de ceux-ci. Bien que les clients puissent considérer ReEncryption un instantané pendant le partage comme une transition essentielle, les instantanés restent immuables du point de vue du client une fois créés.
- **ListSnapshotBlockset** et **GetSnapshotBlock** - Les API EBS Direct sont utilisées pour accéder aux blocs d'instantanés pour un instantané chiffré AWS par clé gérée. Cela est dû au fait que les instantanés chiffrés AWS par clé gérée ne sont pas accessibles autrement entre comptes.
- **Decrypt**- Permet de déchiffrer les instantanés de base chiffrés par clé gérée par le client lorsqu'ils sont téléchargés en mémoire à l'aide des API EBS Direct dans le cadre d'une analyse incrémentielle.
- **ListChangedBlocks**- L'API EBS Direct est utilisée dans le cadre de l'analyse incrémentielle des instantanés pour obtenir la liste des blocs modifiés entre deux instantanés.

- **DescribeKey**- Permet à GuardDuty Malware Protection de déterminer le keyID de la clé AWS gérée dans le compte client.
- **DescribeImages**- Permet de décrire une AMI pour obtenir la liste des instantanés appartenant à l'AMI.
- **DescribeRecoveryPoint**- Permet au service de récupérer les détails du point de restauration et de vérifier le type de ressource pour le point de restauration.
- **CreateBackupAccessPoint, DescribeBackupAccessPoint, DeleteBackupAccessPoint** - Permet au service de créer, de décrire et de supprimer le point d'accès requis pour accéder aux points de restauration.
- **kms:Decrypt**- Permet au service d'accéder aux objets d'un point de restauration S3 lors d'une analyse du point de restauration S3.

Sécuriser le rôle

Le rôle doit être configuré avec une politique de confiance qui approuve le principal du service GuardDuty Malware Protection. Cela garantit qu'aucun principal autre que le GuardDuty service ne peut assumer ce rôle. En outre, nous vous encourageons à limiter les politiques à des ressources spécifiques plutôt qu'à*. Cela inclut les identifiants des instantanés et des clés. Cela garantira que le rôle donne accès uniquement à ces ressources spécifiques.

Important

Une configuration incorrecte peut entraîner des échecs d'analyse en raison d'autorisations insuffisantes.

Comment GuardDuty Malware Protection utilise les subventions dans AWS KMS

GuardDuty La protection contre les programmes malveillants nécessite [des autorisations](#) pour utiliser vos clés KMS.

Lorsque vous lancez une analyse sur un instantané chiffré ou une AMI EC2 composée d'instantanés chiffrés, GuardDuty Malware Protection crée des autorisations en votre nom en envoyant une [CreateGrant](#) demande à AWS KMS. Ces autorisations donnent GuardDuty accès à une clé spécifique de votre compte.

GuardDuty La protection contre les programmes malveillants nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez [DescribeKey](#) des demandes AWS à pour obtenir des informations sur la clé symétrique gérée par le client avec laquelle la ressource soumise pour une analyse des programmes malveillants est cryptée.
- Créez un volume EBS à partir d'un instantané chiffré à l'aide de l'[CreateVolume](#) API et chiffrez-le avec la même clé.
- Accédez aux blocs de snapshots présents sur le snapshot via l'[GetSnapshotBlock](#) API lors d'une analyse incrémentielle.
- Envoyez des demandes de [déchiffrement](#) à AWS KMS pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour lire les données du snapshot pendant le scan.

Vous pouvez révoquer l'autorisation créée ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si vous le faites, vous GuardDuty ne pourrez accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données.

GuardDuty Contexte de chiffrement de la protection contre les

Un [contexte de chiffrement](#) est un ensemble facultatif de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données.

Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS ; lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

GuardDuty Malware Protection utilise l'un des deux contextes de chiffrement.

Contexte de chiffrement 1 : La clé est `aws:guardduty:id`.

```
"encryptionContext": {  
  "aws:guardduty:id": "snap-11112222333344"  
}
```

Ce contexte de chiffrement est utilisé avec les opérations de subvention : `CreateGrant`, `Decrypt`, `GenerateDataKeyWithoutPlaintext`, `ReEncryptTo`, `RetireGrant`, `DescribeKey`.

Une autorisation est créée sur la ressource actuelle avec ce contexte de chiffrement et ces opérations de subvention.

Contexte de chiffrement 2 : la clé est aws:ebs:id

```
"encryptionContext": {  
  "aws:ebs:id": "snap-11112222333344"  
}
```

Ce contexte de chiffrement est utilisé avec les opérations de subvention : ReEncryptFrom, Décrypter, RetireGrant, DescribeKey.

Trois autorisations sont créées avec ces contextes de chiffrement et ces opérations de subvention. Un sur le cliché cible de l'opération de ReEncryptFrom subvention. Un second sur le snapshot cible avec les Decrypt, RetireGrant, DescribeKey opérations. Et une troisième sur l'instantané de base avec les mêmes opérations de subvention que la deuxième subvention.

Autorisations et politique de confiance pour le rôle

Politique d'autorisations

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": [  
      "ebs:ListSnapshotBlocks",  
      "ebs:ListChangedBlocks",  
      "ebs:GetSnapshotBlock"  
    ],  
    "Resource": "arn:aws:ec2:*::snapshot/*"  
  },  
  {  
    "Sid": "CreateGrantPermissions",  
    "Effect": "Allow",  
    "Action": "kms:CreateGrant",  
    "Resource": "arn:aws:kms:*::key/*",  
    "Condition": {  
      "ForAnyValue:StringLike": {  
        "kms:EncryptionContext:aws:guardduty:id": "snap-*",  
        "kms:ViaService": [  
          "guardduty.*.amazonaws.com",  
          "backup.*.amazonaws.com"  
        ]  
      }  
    }  
  }  
],  
}
```

```

        "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
                "Decrypt",
                "CreateGrant",
                "GenerateDataKeyWithoutPlaintext",
                "ReEncryptFrom",
                "ReEncryptTo",
                "RetireGrant",
                "DescribeKey"
            ]
        },
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    },
    {
        "Sid": "CreateGrantPermissionsForReEncryptAndDirectAPIs",
        "Effect": "Allow",
        "Action": "kms:CreateGrant",
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "ForAnyValue:StringLike": {
                "kms:EncryptionContext:aws:ebs:id": "snap-*",
                "kms:ViaService": [
                    "guardduty.*.amazonaws.com",
                    "backup.*.amazonaws.com"
                ]
            }
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
                "Decrypt",
                "ReEncryptTo",
                "ReEncryptFrom",
                "RetireGrant",
                "DescribeKey"
            ]
        },
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
},
{

```

```

    "Effect": "Allow",
    "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
},
{
    "Sid": "ShareSnapshotPermission",
    "Effect": "Allow",
    "Action": [
        "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*"
},
{
    "Sid": "ShareSnapshotKMSPermission",
    "Effect": "Allow",
    "Action": [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
    ],
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "ec2.*.amazonaws.com"
        }
    }
},
{
    "Sid": "DescribeKeyPermission",
    "Effect": "Allow",
    "Action": "kms:DescribeKey",
    "Resource": "arn:aws:kms:*:*:key/*"
},
{
    "Sid": "DescribeRecoveryPointPermission",
    "Effect": "Allow",
    "Action": [
        "backup:DescribeRecoveryPoint"
    ],
    "Resource": "*"
},
{

```

```

        "Sid": "CreateBackupAccessPointPermissions",
        "Effect" : "Allow",
        "Action" : [
            "backup:CreateBackupAccessPoint"
        ],
        "Resource": "arn:aws:backup:*:*:recovery-point:*"
    },
    {
        "Sid": "ReadAndDeleteBackupAccessPointPermissions",
        "Effect" : "Allow",
        "Action" : [
            "backup:DescribeBackupAccessPoint",
            "backup>DeleteBackupAccessPoint"
        ],
        "Resource": "*"
    },
    {
        "Sid": "KMSKeyPermissionsForInstantAccess",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "backup.*.amazonaws.com"
            }
        }
    }
]
}

```

Politique de confiance

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guarddduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

```
}  
]  
}
```

(Facultatif) Commencez à utiliser Malware Protection for Backup Independently (console uniquement)

Utilisez cette étape facultative lorsque vous souhaitez commencer à utiliser l'option de détection des menaces Malware Protection for Backup, quel que soit le GuardDuty statut de votre AWS compte.

Si vous souhaitez également utiliser d'autres plans de protection dédiés GuardDuty, vous devez commencer par utiliser le GuardDuty service Amazon. Pour plus d'informations sur les plans de GuardDuty protection, consultez la section [Fonctionnalités de GuardDuty](#).

Étapes pour démarrer avec Malware Protection for Backup

1. Connectez-vous à la console de AWS gestion et ouvrez la <https://console.aws.amazon.com/guardduty/console> à l'adresse <https://console.aws.amazon.com/guardduty/>
2. Sélectionnez Découvrir les fonctionnalités de protection contre les logiciels malveillants et cliquez sur Commencer.
3. En cliquant sur Get Started, vous pouvez choisir entre des options telles que les fonctionnalités AWS Backup et S3 Malware Protection.

Malware Protection Info

Use threat detection capabilities in GuardDuty to analyze your AWS environment and identify malware. Configure one or more malware scanning features based on your security needs. [AWS Service Terms for GuardDuty Malware Protection](#) will apply. Scanning cost will apply. [View pricing](#)

AWS Backup - new

Scan AWS Backup recovery points and backup data across Amazon EC2, Amazon EBS, and Amazon S3 resources to detect malware and identify the last known clean backup. Configure automatic malware scanning in your backup plans or run on-demand scans. [Learn more](#)

[View feature](#)

S3

Automatically scan new files uploaded to your selected Amazon S3 buckets and object prefixes to detect malware. [Learn more](#)

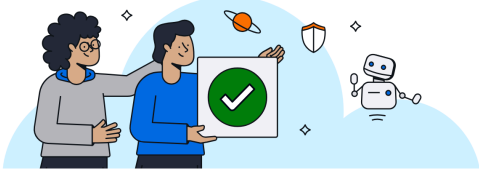
Status

⊖ Not enabled

[View feature](#)

4. Vous êtes redirigé vers la page Malware Protection for Backup, où vous pouvez choisir de démarrer une analyse à la demande ou de Afficher les analyses de logiciels malveillants.

Malware Protection for AWS Backup - new [Info](#)
[AWS Service Terms for GuardDuty Malware Protection](#) [L2](#) will apply. Malware detection from scanning cost will apply. [View pricing](#) [L2](#)



Detect malware in your backup data
Integrate with AWS Backup to scan backups and recovery points across Amazon EC2, Amazon EBS, and Amazon S3 resources. When GuardDuty detects malware, you can restore to the last known clean backup in AWS Backup.
To get started, enable malware scanning in your new and existing backup plans. [Learn more](#) [L2](#)
[Start with AWS Backup](#) [L2](#)

Explore capabilities

Malware scan results
Monitor the progress of both automatic and on-demand scans of your backups. Access detailed scan results in GuardDuty.
[View malware scans](#)

Investigate malware findings
Provides comprehensive threat information from scans of your backup resources, helping you quickly identify and respond to potential threats in your stored data.
[View all findings](#)

On-demand scanning mode
Start full or incremental scans of your backup data anytime from GuardDuty. Run scans to meet compliance requirements or verify backup contents.
[Start on-demand scan](#)

Cross-account monitoring with AWS Organizations
Strengthen your organization's security posture by monitoring malware threats across throughout your backup environment. [Learn more](#) [L2](#)



Lancement d'un On-Demand scan de protection contre les logiciels malveillants pour Backup

Console

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Accédez à Malware Protection for Backup et cliquez sur Démarrer le scan à la demande.
3. Choisissez entre le scan complet et le scan incrémentiel.
 1. Pour démarrer une analyse complète, entrez l'ARN de la ressource à analyser.
 2. Pour une analyse incrémentielle, entrez l'ARN de la ressource cible et l'ARN de la ressource de référence.
 3. Si la ressource analysée est un point de restauration, vous devez également saisir le nom du AWS Backup Vault auquel elle appartient.
 4. Pour une ressource S3 PITR, transmettez un horodatage de fin. L'horodatage de fin ne peut pas être antérieur à (heure actuelle - 15 minutes).

4. Accès au service : vous devez choisir un rôle disposant des autorisations requises pour accéder à la ressource et effectuer l'analyse. Cliquez sur Afficher la politique pour afficher les autorisations exactes requises pour le rôle, ainsi que la politique de confiance requise.

Vous pouvez apporter des modifications à la politique en fonction de vos besoins ou limiter les autorisations à la ressource exacte. Pour plus de détails sur la création ou la mise à jour d'un rôle IAM, consultez [GuardDuty Protection contre les logiciels malveillants pour les sauvegardes : autorisations relatives aux rôles IAM](#).

Pour les problèmes liés aux autorisations des rôles IAM, consultez la section [Résolution des erreurs liées aux autorisations des rôles IAM](#).

API/CLI

Invoquez [StartMalwareScan](#) qui accepte `resourceArn` la ressource pour laquelle vous souhaitez lancer une analyse des programmes malveillants à la demande. Si vous souhaitez démarrer une analyse incrémentielle, transmettez `baselineResourceArn.incrementalScanDetails`. Dans le cadre de la configuration du scan, vous devez également fournir un rôle IAM disposant de toutes les autorisations nécessaires pour démarrer le scan. Si la ressource analysée est une ressource S3 PITR, vous devez transmettre un horodatage de fin. Une fois que vous avez lancé une analyse avec succès, `StartMalwareScan` renvoie `unscanId`. Appelez `GetMalwareScanAPI` pour suivre la progression de l'analyse démarrée et pour obtenir les détails de l'analyse une fois celle-ci terminée.

Surveillance de l'état des scans et des résultats de la protection contre les logiciels malveillants pour Backup

Après le lancement d'une analyse des logiciels malveillants, GuardDuty fournit quelques mécanismes grâce auxquels vous pouvez surveiller l'état et le résultat d'une analyse. Le tableau suivant fournit certaines des valeurs associées aux analyses de programmes malveillants.

Valeurs potentielles

RUNNING, COMPLETED , COMPLETED_WITH_ISSUES , FAILED ou SKIPPED

Valeurs potentielles

FULL_SCAN ou INCREMENTAL_SCAN

GUARDDUTY_INITIATED , ON_DEMAND ou BACKUP_INITIATED

NO_THREATS_FOUND ou THREATS_FOUND

*Notez que l'état des résultats du scan peut ne pas être présent si le scan n'est pas terminé. L'état des résultats du scan de THREATS_FOUND indique que la présence d'un GuardDuty logiciel malveillant a été détectée.

Pour les points de restauration S3, COMPLETED_WITH_ISSUES indique que certains fichiers ont été ignorés ou ont échoué. Pour les AMI, COMPLETED_WITH_ISSUES indique qu'au moins un instantané n'a pas pu être numérisé. Voir ci-dessous la liste des raisons ignorées.

Les scans peuvent également être ignorés pour diverses raisons. Le tableau ci-dessous explique les raisons pour lesquelles les scans peuvent être ignorés :

Raison

Le rôle du client ne dispose pas des autorisations requises pour que le service effectue l'analyse

Raison

La ressource qui tente d'être scannée n'existe pas dans le compte ou a été supprimée lors de la numérisation

La taille de l'instantané est supérieure à celle actuellement prise en charge par GuardDuty

Les ressources spécifiées dans la demande d'analyse incrémentielle n'ont aucune différence

La ressource n'est pas dans l'état attendu. Si l'analyse est incrémentielle, le point de restauration de base n'est pas à l'état DISPONIBLE ou TERMINÉ

Pour les analyses incrémentielles, la ressource de base et la ressource actuelle ne proviennent pas de la même lignée

Pour les analyses incrémentielles, la ressource de base n'a pas été scannée précédemment ou aucune analyse terminée n'a été trouvée

Raison

Pour les analyses incrémentielles, la date de création de la ressource de base est supérieure à la date de création de la ressource actuelle

Le type de ressource demandé ne prend pas en charge l'analyse incrémentielle

Les AMI publiques, les AMI ne disposant que d'un stockage éphémère et les AMI non disponibles ne sont pas éligibles à la numérisation

Les instantanés stockés à froid ne sont pas éligibles à la numérisation

La numérisation n'est pas prise en charge pour les types de ressources composites

La ressource demandée contient un code produit Amazon Marketplace qui ne prend pas en charge la numérisation

Raison

Les AMI ne prennent pas en charge l'analyse de plus de 40 instantanés

Aucun mappage de périphérique de bloc Ebs n'a été trouvé pour la ressource demandée

Pour les analyses incrémentielles, l'arn de la ressource de base est différent de l'arn de la ressource attendue

Tous les fichiers de l'analyse ont été ignorés ou ont échoué

Les résultats du scan ont une période de conservation de 90 jours. Choisissez votre méthode d'accès préférée pour suivre l'état de votre analyse des logiciels malveillants.

Surveillance des scans à l'aide de la console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Analyses des logiciels malveillants.

3. Vous pouvez filtrer les analyses de programmes malveillants à l'aide des propriétés suivantes disponibles dans la barre de recherche du filtre.
- ID de scan — Identifiant unique associé à l'analyse des programmes malveillants.
 - ID de compte : compte sur lequel l'analyse des logiciels malveillants a été lancée.
 - ARN de ressource : nom de ressource Amazon (ARN) associé à la ressource Amazon associée au scan.
 - Type de ressource : type de ressource associé à l'analyse, tel qu'une instance EC2, un instantané EBS | AMI EC2, un point de restauration EBS, un point de restauration EC2 ou un point de restauration S3.
 - État : état de l'analyse, tel que En cours, ignoré, terminé, terminé avec des problèmes ou échec.
 - Type de scan : indique s'il s'agit d'un On-demand scan ou GuardDuty-initiated d'un scan Backup-Initiated anti-malware.

Surveillance des scans à l'aide du API/CLI

- Vous pouvez invoquer `ListMalwareScans` pour filtrer les analyses de programmes malveillants par `RESOURCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS`, `RESOURCE_TYPE`, et `SCAN_START_TIME`. Vous pouvez également appeler `GetMalwareScan` pour récupérer des métadonnées plus détaillées d'une analyse en fournissant un identifiant de numérisation en entrée. Les critères de `GUARDDUTY_FINDING_ID` filtrage sont disponibles lorsque le `SCAN_TYPE` est GuardDuty lancé.
- Vous pouvez modifier l'exemple *filter-criteria* dans la commande ci-dessous et filtrer un `CriterionKey` par un. Les options pour `CriterionKey` sont `Resource_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS`, `RESOURCE_TYPE`, et `SCAN_START_TIME`. Vous pouvez modifier le *max-results* (jusqu'à 50) et le *sort-criteria*. Le `AttributeName` champ est obligatoire pour *sort-criteria* et doit être défini sur `scanStartTime`. Dans l'exemple suivant, les valeurs indiquées *red* sont des espaces réservés. Remplacez-les par les valeurs correspondant à votre compte. Si vous utilisez le même `CriterionKey` que ci-dessous pour `ListMalwareScans`, assurez-vous de remplacer l'exemple `EqualsValue` par celui par lequel *resource-type* vous souhaitez filtrer.

```
aws guardduty list-malware-scans --max-results 25 --sort-criteria  
'{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
```

```
'{"FilterCriterion":[{"CriterionKey":"RESOURCE_TYPE", "FilterCondition":  
{"EqualsValue":"EBS_SNAPSHOT"}]} ]'
```

```
aws guardduty get-malware-scan --scan-id abc123
```

- La réponse à la commande ci-dessus pour ListMalwareScans renverra jusqu'à 25 scans avec quelques détails sur les ressources affectées. La réponse à la commande ci-dessus pour GetMalwareScan renverra un scan unique avec des métadonnées détaillées sur le scan.

Surveillance des scans à l'aide de EventBridge

Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications Software-as-a-Service (SaaS) et services Amazon et achemine ces données vers des cibles telles que Lambda. Cela vous permet de surveiller les événements qui se produisent dans les services et de créer des architectures basées sur les événements. Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

GuardDuty publie EventBridge des notifications sur le bus d'événements par défaut une fois que l'état du scan est déterminé. Vous pouvez configurer des EventBridge règles dans votre compte pour envoyer des événements à d'autres services intégrés à Amazon EventBridge. La EventBridge tarification standard s'appliquera. Pour plus d'informations, consultez les [EventBridge tarifs Amazon](#).

La plupart des valeurs indiquées ci-dessous sont des espaces réservés pour l'exemple et varient en fonction du scan.

Événements liés aux résultats du scan des programmes malveillants

Valeurs de type de détail potentielles pour Backup :

- « Résultat de l'analyse instantanée EBS GuardDuty Malware Protection »
- « Résultat de l'analyse de l'AMI EC2 GuardDuty Malware Protection »
- « Résultat du scan de GuardDuty Malware Protection S3 Recovery Point »
- « Résultat de l'analyse EBS Recovery Point contre les GuardDuty malwares »
- « Résultat du scan EC2 Recovery Point de protection contre les GuardDuty malwares »

Exemple de modèle d'événement :

```
{
  "detail-type": ["GuardDuty Malware Protection EC2 AMI Scan Result"],
  "source": ["aws.guarddduty"]
}
```

Exemple de schéma de notification pour le scan d'une AMI EC2 sans détection de menaces :

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
  "source": "aws.guarddduty",
  "account": "1111222233334444",
  "time": "2025-11-01T00:00:00Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/ami-1234567890abcdef0"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "EC2_AMI",
    "scanId": "d41d8cd98f00b204e9800998ecf8427e",
    "scanStatusReason": null,
    "scanType": "ON_DEMAND",
    "triggerType": "GUARDDUTY",
    "scanCategory": "FULL_SCAN",
    "scanStartTime": 1234567890123,
    "scanCompleteTime": 2345678901234,
    "scanResultDetails": {
      "scanResultStatus": "NO_THREATS_FOUND",
      "uniqueThreatCount": null
    }
  }
}
```

Exemple de schéma de notification pour le scan de l'AMI EC2 en cas de détection de menaces :

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
  "source": "aws.guarddduty",

```

```

"account": "1111222233334444",
"time": "2025-11-01T00:00:00Z",
"region": "us-east-1",
"resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/ami-1234567890abcdef0"],
"detail": {
  "schemaVersion": "1.0",
  "scanStatus": "COMPLETED",
  "resourceType": "EC2_AMI",
  "scanId": "d41d8cd98f00b204e9800998ecf8427e",
  "scanStatusReason": null,
  "scanType": "ON_DEMAND",
  "triggerType": "GUARDDUTY",
  "scanCategory": "FULL_SCAN",
  "scanStartTime": 1234567890123,
  "scanCompleteTime": 2345678901234,
  "scanResultDetails": {
    "scanResultStatus": "THREATS_FOUND",
    "uniqueThreatCount": 1,
    "threats": {
      "name": "EICAR-Test-File (not a virus)",
      "source": "AMAZON",
      "count": 2,
      "itemDetails": [{
        "resourceArn": "arn:aws:ec2:us-east-1:1111222233334444:snapshot/snap-abcdef01234567890",
        "hash":
"e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855",
        "itemPath": "/eicar.txt",
        "additionalInfo": {
          "versionId": null,
          "deviceName": "/dev/sdf"
        }
      }]
    }
  }
}

```

Exemple de schéma de notification pour un scan d'AMI EC2 ignoré :

```

{
  "version": "0",

```

```
"id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
"detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
"source": "aws.guardduty",
"account": "1111222233334444",
"time": "2025-11-01T00:00:00Z",
"region": "us-east-1",
"resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/ami-1234567890abcdef0"],
"detail": {
  "schemaVersion": "1.0",
  "scanStatus": "SKIPPED",
  "resourceType": "EC2_AMI",
  "scanId": "d41d8cd98f00b204e9800998ecf8427e",
  "scanStatusReason": "UNSUPPORTED_AMI",
  "scanType": "ON_DEMAND",
  "triggerType": "GUARDDUTY",
  "scanCategory": "FULL_SCAN",
  "scanStartTime": 1234567890123,
  "scanCompleteTime": 2345678901234,
  "scanResultDetails": {
    "uniqueThreatCount": null,
    "threats": null
  }
}
```

Quotas pour la protection contre les logiciels malveillants lors de la sauvegarde

Protection contre les malwares pour les quotas de sauvegarde

Nom du quota	AWS valeur de quota par défaut	Est-il ajustable ?	Description
StartMalwareScan Limite TPS pour tous les types de ressources	10	Non	
Taille maximale de capture d'écran prise en charge	2 Tio	Non	Cette limite s'applique à la taille complète de l'instantané (fullSnapshotSizeIn

Nom du quota	AWS valeur de quota par défaut	Est-il ajustable ?	Description
			<p>Bytes), et non à la taille incrémentielle de l'instantané.</p> <p>Pour plus d'informations, consultez Snapshot dans le manuel Amazon EC2 API Reference.</p> <p>Dans le cas d'un scan incrémentiel, GuardDuty ignore le scan si le cliché actuel ou le cliché de base dépasse cette limite.</p>
Systèmes de fichiers pris en charge pour les scans de snapshots et d'AMI	<ul style="list-style-type: none"> • New Technology File System (NTFS) • X File System (XFS) • Second extended (ext2) File System • Fourth extended (ext4) File System • File Allocation Table (FAT) File System • Virtual File Allocation Table (VFAT) File System 	Non	

Nom du quota	AWS valeur de quota par défaut	Est-il ajustable ?	Description
Nombre maximal de snapshots pris en charge par une AMI pour l'analyse des programmes malveillants	40 pour un scan complet. S'il y en a plus de 40, il n'en GuardDuty analysera que 40 parmi tous les instantanés. Dans le cas d'une analyse incrémentielle, la numérisation est ignorée.	Non	
Taille maximale d'un objet dans un point de restauration S3	100 Go	Non	Taille maximale de l'objet S3 qui GuardDuty tentera de détecter les logiciels malveillants.
Octets d'archive extraits	100 Go	Non	<p>Quantité maximale de données GuardDuty pouvant être extraites et analysées à partir d'un fichier d'archive.</p> <p>GuardDuty ignorera l'extraction des fichiers d'archive sur une taille supérieure à 100 Go.</p>

Nom du quota	AWS valeur de quota par défaut	Est-il ajustable ?	Description
Fichiers d'archives extraits	10 000	Non	<p>Nombre maximal de fichiers GuardDuty pouvant être extraits et analysés dans un fichier d'archive. Si l'archive contient plus de 10 000 fichiers, vous GuardDuty devrez ignorer le fichier archivé.</p> <div><p> Note</p><p>Les types de fichiers composés sont potentiellement soumis à ces limites. Les types de fichiers incluent, sans s'y limiter, les messages électroniques codés MIME (Multipurpose Internet Mail Extensions), les fichiers Python compilés (PYC), les fichiers d'aide HTML compilés (CHM), tous les programmes d'installation et les documents OpenDocument Format (ODF).</p></div>
Niveaux de profondeur d'archivage maximaux	5	Non	Les niveaux maximaux d'archives imbriquées GuardDuty pouvant être extraites. Si l'archive inclut des fichiers imbriqués au-delà de cette valeur, ces fichiers imbriqués GuardDuty seront ignorés.

GuardDuty Protection RDS

Note

Vous pouvez configurer la protection RDS ainsi que tous les autres plans de protection à partir d'une seule page de la GuardDuty console. Pour plus d'informations, consultez [Configuration des plans de protection](#).

Dans Amazon, RDS Protection GuardDuty analyse et établit le profil des connexions RDS et de l'activité des données afin de détecter les menaces potentielles pesant sur vos bases de données Amazon Aurora et RDS pour PostgreSQL.

[RDS Protection for login activity analyse les événements de connexion pour détecter les menaces d'accès potentielles aux bases de données Amazon Aurora \(Amazon Aurora MySQL-Compatible Edition et Aurora PostgreSQL-Compatible Edition\), RDS pour PostgreSQL, Amazon RDS pour MySQL et Amazon RDS pour MariaDB](#). Il vous aide à identifier les comportements de connexion potentiellement suspects sur ces bases de données prises en charge. GuardDuty surveille et établit des profils en permanence [Activité de connexion RDS](#) pour détecter toute activité anormale. Par exemple, un acteur externe invisible a un accès non autorisé à votre base de données, ou un adversaire tente d'y accéder par force brute en devinant le mot de passe de la base de données.

RDS Protection for data activity analyse les modèles de requêtes de base de données sur les bases de données [Amazon Aurora](#) pour PostgreSQL et [RDS pour PostgreSQL](#) afin de détecter les menaces potentielles d'accès et de manipulation des données. GuardDuty surveille et établit en permanence le profil [Activité des données RDS](#) des comportements anormaux. Par exemple, un acteur lit beaucoup plus de lignes que d'habitude pour cette base de données ou cet utilisateur, supprime ou supprime des données, ou accède à votre base de données à partir d'un maliciel connu ou d'une adresse IP Tor.

Pour les comptes qui n'ont pas encore activé la protection RDS, vous pouvez en savoir plus sur cette fonctionnalité [30-day free trial](#) et choisir de l'activer. Pour activer cette fonctionnalité, consultez [Activation de la protection RDS dans les environnements à comptes multiples](#) ou [Activation de la protection RDS pour un compte autonome](#).

 Remarque

Les instances de réplication en lecture de RDS pour PostgreSQL nécessitent que l'instance de base de données principale utilise une version de base de données prise en charge et qu'elle soit correctement répliquée à partir de la base de données principale. Pour plus d'informations sur les répliques de lecture, consultez la section [Utilisation des répliques de lecture d'instances de base de données dans le guide](#) de l'utilisateur Amazon RDS.

La protection RDS ne nécessite aucune infrastructure supplémentaire ; elle est conçue de manière à ne pas affecter les performances de vos instances de base de données. Lorsque RDS Protection détecte une tentative de connexion potentiellement suspecte ou anormale, une exfiltration ou une activité destructrice de données, GuardDuty génère une ou plusieurs informations détaillées sur la base [Types de résultat de la protection RDS](#) de données potentiellement compromise.

essai gratuit de 30 jours

- Lorsque vous l'activez GuardDuty Compte AWS dans une nouvelle région pour la première fois, vous bénéficiez d'un essai gratuit de 30 jours. Dans ce cas, active GuardDuty également la protection RDS, qui est incluse dans l'essai gratuit. La surveillance de l'activité de connexion RDS Protection et la surveillance de l'activité des données de RDS Protection commenceront à surveiller l'activité de vos bases de données.
- Lorsque vous utilisez déjà GuardDuty et décidez d'activer la protection RDS dans une nouvelle région pour la première fois, votre compte dans cette région bénéficiera d'un essai gratuit de 30 jours pour RDS Protection.
- Lorsque vous utilisez déjà RDS Protection pour vos activités de connexion à un Compte AWS et que vous décidez d'activer RDS Protection pour l'activité liée aux données pour la première fois, votre compte bénéficiera d'un essai gratuit de 30 jours de RDS Protection pour les activités liées aux données.
- Vous pouvez choisir de désactiver la surveillance de l'activité des données RDS Protection ou RDS Protection dans n'importe quelle région à tout moment.
- Au cours de l'essai gratuit de 30 jours, vous pouvez obtenir une estimation de vos coûts d'utilisation pour ce compte et cette région. Après la fin de l'essai gratuit de 30 jours, la protection RDS n'est pas automatiquement désactivée. Votre compte dans cette région commencera à entraîner des frais d'utilisation. Pour plus d'informations, consultez [Surveillance de GuardDuty l'utilisation et estimation des coûts](#).

Lorsque la fonction de protection RDS n'est pas activée, GuardDuty elle ne détecte aucun comportement de connexion ou de données anormal ou suspect. Si vous désactivez la protection RDS, la surveillance de l'activité RDS s'arrête. GuardDuty immédiatement, ne détectera aucune menace potentielle pour vos instances de base de données prises en charge et ne générera aucun type de recherche associé.

Pour savoir Régions AWS où les bases de données Aurora PostgreSQL Limitless sont prises en charge, consultez la section Exigences relatives à la base de données [Aurora](#) PostgreSQL Limitless.

Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge

Le tableau suivant indique les versions de base de données Aurora et Amazon RDS prises en charge pour la surveillance de l'activité de connexion et de l'activité des données par RDS Protection. GuardDuty pourrait être étendu à d'autres bases de données Amazon RDS à l'avenir.

Moteur de base de données Amazon Aurora et Amazon RDS	Versions du moteur prises en charge par la surveillance de l'activité	Versions du moteur compatibles avec la surveillance de l'activité des données
Aurora MySQL	<ul style="list-style-type: none"> Versions 2.10.2 ou ultérieures Versions 3.02.1 ou ultérieures Versions majeures suivantes 	Non pris en charge
Aurora PostgreSQL	<ul style="list-style-type: none"> 10.23 ou version ultérieure Versions 11.12 ou ultérieures Versions 12.7 ou ultérieures Versions 13.3 ou ultérieures Versions 14.3 ou ultérieures 15.2 ou version ultérieure 16.1 ou version ultérieure 	<ul style="list-style-type: none"> 11.19 ou version ultérieure 12.14 ou version ultérieure 13.10 ou version ultérieure 14.7 ou version ultérieure 15.2 ou version ultérieure Versions majeures suivantes

Moteur de base de données Amazon Aurora et Amazon RDS	Versions du moteur prises en charge par la surveillance de l'activité	Versions du moteur compatibles avec la surveillance de l'activité des données
	<ul style="list-style-type: none"> Versions majeures suivantes 	
RDS pour PostgreSQL	<ul style="list-style-type: none"> 11.17 ou version ultérieure 12.12 ou version ultérieure 13.8 ou version ultérieure 14.5 ou version ultérieure RDS pour PostgreSQL version 15 RDS pour PostgreSQL version 16 RDS pour PostgreSQL version 17 RDS pour PostgreSQL version 18 Versions majeures suivantes 	<ul style="list-style-type: none"> 11.20 ou version ultérieure 12h15 ou version ultérieure 13.11 ou version ultérieure 14.8 ou version ultérieure 15.3 ou version ultérieure Versions majeures suivantes
Base de données Amazon Aurora PostgreSQL Limitless	<ul style="list-style-type: none"> 16.4-limitless Versions majeures suivantes 	Non pris en charge
Amazon RDS for MariaDB	<ul style="list-style-type: none"> 10.6.25 ou version ultérieure 10.11.16 ou version ultérieure 11.4.10 ou version ultérieure 11.8.6 ou version ultérieure Versions majeures suivantes 	Non pris en charge

Moteur de base de données Amazon Aurora et Amazon RDS	Versions du moteur prises en charge par la surveillance de l'activité	Versions du moteur compatibles avec la surveillance de l'activité des données
Amazon RDS for MySQL	<ul style="list-style-type: none"> 8.0.45 ou version ultérieure 8.4.8 ou version ultérieure Versions majeures suivantes 	Non pris en charge

Activité de connexion RDS

Lorsque vous activez la fonction de protection RDS, commence GuardDuty automatiquement à surveiller l'activité de connexion RDS pour vos bases de données, directement depuis les services Aurora et Amazon RDS. L'activité de connexion RDS capture les tentatives de connexion réussies et infructueuses effectuées [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) dans votre AWS environnement. En cas d'indication d'un comportement de connexion anormal, GuardDuty génère un résultat contenant des informations détaillées sur la base de données potentiellement compromise. Lorsque vous activez la protection RDS pour la première fois ou que vous avez une instance de base de données nouvellement créée, une période d'apprentissage est prévue pour définir un comportement normal. Pour cette raison, il est possible que les instances de base de données nouvellement activées ou nouvellement créées ne soient associées à aucune anomalie de connexion pendant deux semaines au maximum.

Lorsque RDS Protection détecte une menace potentielle, telle qu'un schéma inhabituel dans une série de tentatives de connexion réussies, échouées ou incomplètes, en GuardDuty génère une ou plusieurs [Types de résultat de la protection RDS](#). Selon le type de découverte, il peut inclure des détails sur le comportement anormal, tels que [Anomalies basées sur l'activité de connexion RDS](#). GuardDuty ne met pas à votre disposition les journaux d'activité de connexion RDS.

Activité des données RDS

Lorsque vous activez la protection RDS pour l'activité des données, GuardDuty analyse les modèles d'activité des bases de données dans les bases de données Aurora et Amazon RDS prises en charge afin d'identifier les menaces potentielles d'accès et de manipulation des données. S'il détecte une activité anormale sur les données, il GuardDuty génère une constatation contenant des détails sur la base de données potentiellement compromise. Lorsque vous activez la protection RDS pour

l'activité liée aux données pour la première fois, ou lorsque vous créez une nouvelle instance de base de données, une période d'apprentissage d'une durée maximale de deux semaines est prévue pour établir une base de référence de comportement normal. Pendant cette période, il se peut qu'aucune activité anormale sur les données ne soit détectée.

Lorsque RDS Protection for Data Activity détecte une menace potentielle, elle en GuardDuty génère une ou plusieurs [Types de résultat de la protection RDS](#). Par exemple, un acteur lit beaucoup plus de lignes que d'habitude pour cette base de données ou cet utilisateur, supprime ou supprime des données, ou accède à votre base de données à partir d'une adresse IP malveillante ou Tor connue. Selon le type de découverte, la découverte peut inclure des détails sur le comportement anormal, tels que [Anomalies liées à l'activité des données RDS](#). GuardDuty ne met pas les journaux d'activité des données RDS à votre disposition.

Activation de la protection RDS dans les environnements à comptes multiples

Dans un environnement à comptes multiples, seul le compte GuardDuty administrateur délégué a la possibilité d'activer ou de désactiver la fonctionnalité de protection RDS, y compris la configuration supplémentaire de surveillance de l'activité des données RDS, pour les comptes des membres de son organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Ce compte d' GuardDuty administrateur délégué peut choisir d'activer automatiquement la surveillance de l'activité de connexion RDS et la surveillance de l'activité des données RDS pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements à comptes multiples, consultez. [Gestion de plusieurs comptes](#)

Activation de la protection RDS pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour activer la protection RDS, y compris la configuration supplémentaire de surveillance de l'activité des données RDS, pour le compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Plans de protection.

3. Choisissez Configurer toutes les activations.
4. Sous Protection RDS, recherchez les entrées RDS Login Activity Monitoring et RDS Data Activity Monitoring.
5. Dans la colonne Ce compte, choisissez Activé pour chaque entrée que vous souhaitez activer ou Non activé pour la désactiver.

 Note

La surveillance de l'activité de connexion RDS doit être activée pour que vous puissiez activer la surveillance de l'activité des données RDS.

API/CLI

Exécutez l'opération [updateDetector](#) API en utilisant votre propre identifiant de détecteur régional et en transmettant l'features objet name sous RDS_LOGIN_EVENTS et en status tant que ENABLED. Pour activer également la surveillance de l'activité des données RDS, passez RDS_DATA_RISK en name dessous AdditionalConfiguration avec status défini sur. ENABLED

Vous pouvez également utiliser AWS CLI pour activer la protection RDS. Exécutez la commande suivante et remplacez-la `12abc34d567e8fa901bc2d34e56789f0` par l'ID du détecteur de votre compte et `us-east-1` par la région dans laquelle vous souhaitez activer la protection RDS.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active la surveillance de l'activité de connexion RDS sur le compte administrateur délégué et permet également d'activer la surveillance de l'activité des données RDS : AdditionalConfiguration

```
aws guardduty update-detector \  
  --detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
  --region us-east-1 \  
  --features '[  
    {  
      "Name": "RDS_LOGIN_EVENTS",  
      "Status": "ENABLED",
```

```
"AdditionalConfiguration": [  
  {  
    "Name": "RDS_DATA_RISK",  
    "Status": "ENABLED"  
  }  
]  
'
```

Auto-enable Protection RDS pour tous les comptes membres

Choisissez votre méthode d'accès préférée pour activer la fonctionnalité de protection RDS, y compris la configuration supplémentaire de surveillance de l'activité des données RDS, pour tous les comptes membres. Cela inclut les comptes membres existants et les nouveaux comptes qui rejoignent l'organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations.
4. Sous Protection RDS, choisissez Activer pour tous les comptes. Cette action active automatiquement la protection RDS pour les comptes existants et nouveaux de l'organisation.
5. Pour activer également la surveillance de l'activité des données RDS pour chaque compte, développez la section Configuration supplémentaire et choisissez Activer pour tous les comptes pour la surveillance de l'activité des données RDS.
6. Choisissez Enregistrer tout, puis cliquez sur Confirmer et enregistrez.

Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

API/CLI

Pour activer la protection RDS pour tous les comptes membres de votre organisation, y compris les membres existants et les nouveaux comptes qui se joindront ultérieurement, appelez l'opération [UpdateOrganizationConfiguration](#) API en utilisant la votre *detector ID*. Définissez sur `AutoEnable` `ALL` pour la `RDS_LOGIN_EVENTS` fonctionnalité et passez `RDS_DATA_RISK` en dessous `AdditionalConfiguration` avec `AutoEnable` set `ALL` to pour activer également automatiquement la surveillance de l'activité des données RDS.

Vous pouvez également utiliser AWS CLI pour activer la protection RDS. Exécutez la commande suivante et remplacez-la `12abc34d567e8fa901bc2d34e56789f0` par l'ID du détecteur de votre compte et `us-east-1` par la région dans laquelle vous souhaitez activer la protection RDS.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active automatiquement les deux comptes membres de l'organisation `RDS_LOGIN_EVENTS` et `RDS_DATA_RISK` pour chacun d'entre eux :

```
aws guardduty update-organization-configuration \
  --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
  --region us-east-1 \
  --auto-enable-organization-members ALL \
  --features '[
    {
      "Name": "RDS_LOGIN_EVENTS",
      "AutoEnable": "ALL",
      "AdditionalConfiguration": [
        {
          "Name": "RDS_DATA_RISK",
          "AutoEnable": "ALL"
        }
      ]
    }
  ]'
```

Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Activer la protection RDS pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la protection RDS, y compris la configuration supplémentaire de surveillance de l'activité des données RDS, pour tous les comptes de membres actifs existants de votre organisation. Les comptes de membres déjà GuardDuty activés sont appelés membres actifs existants.

Note

La surveillance de l'activité de connexion RDS doit être activée sur un compte membre pour que vous puissiez activer la surveillance de l'activité des données RDS sur ce compte.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sur la page Comptes, sélectionnez les comptes de membres actifs existants que vous souhaitez activer. Pour sélectionner tous les comptes, utilisez la case à cocher dans l'en-tête du tableau.
4. Dans le menu déroulant Modifier les plans de protection, choisissez RDS Login Activity, puis sélectionnez Activer.
5. Pour activer également la surveillance de l'activité des données RDS sur les comptes sélectionnés, ouvrez à nouveau le menu déroulant Modifier les plans de protection, choisissez Activité des données RDS, puis sélectionnez Activer. La surveillance de l'activité de connexion RDS doit déjà être activée sur chaque compte sélectionné.

API/CLI

Exécutez l'opération d'[updateMemberDetectors](#)API en utilisant la votre *detector ID*. Passez RDS_DATA_RISK en revue AdditionalConfiguration la RDS_LOGIN_EVENTS fonctionnalité pour contrôler également la surveillance de l'activité des données RDS.

Vous pouvez également utiliser AWS CLI pour activer la protection RDS. Exécutez la commande suivante et remplacez-la `12abc34d567e8fa901bc2d34e56789f0` par l'ID du détecteur de votre compte et `us-east-1` par la région dans laquelle vous souhaitez activer la protection RDS.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

L'exemple suivant active la surveillance de l'activité de connexion RDS sur un compte de membre actif existant, et l'utilise AdditionalConfiguration pour activer également la surveillance de l'activité des données RDS :

```
aws guardduty update-member-detectors \
  --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
  --region us-east-1 \
  --account-ids 111122223333 \
  --features '[
    {
      "Name": "RDS_LOGIN_EVENTS",
      "Status": "ENABLED",
      "AdditionalConfiguration": [
        {
          "Name": "RDS_DATA_RISK",
          "Status": "ENABLED"
        }
      ]
    }
  ]'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Auto-enable Protection RDS pour les nouveaux comptes de membres

Choisissez votre méthode d'accès préférée pour activer la surveillance de l'activité de connexion RDS et la surveillance de l'activité des données RDS pour les nouveaux comptes qui rejoignent votre organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations.
4. Choisissez Configurer les comptes manuellement.
5. Sous Protection RDS, sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la protection RDS sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
6. Pour également activer automatiquement la surveillance de l'activité des données RDS pour les nouveaux comptes, sélectionnez Configuration supplémentaire et sélectionnez Activer automatiquement pour les nouveaux comptes membres pour la surveillance de l'activité des données RDS.
7. Cliquez sur Enregistrer.

API/CLI

Pour activer automatiquement la protection RDS pour les nouveaux comptes qui rejoignent votre organisation, appelez l'opération d'[UpdateOrganizationConfiguration](#) API en utilisant la vôtre.

detector ID Définissez sur `AutoEnable NEW` pour la `RDS_LOGIN_EVENTS` fonctionnalité et passez `RDS_DATA_RISK` en dessous `AdditionalConfiguration` avec `AutoEnable` set `NEW` to pour activer également automatiquement la surveillance de l'activité des données RDS. Pour arrêter l'activation automatique d'une fonctionnalité pour les nouveaux comptes, définissez sa `AutoEnable` valeur sur `NONE`.

Vous pouvez également utiliser AWS CLI pour activer la protection RDS. Exécutez la commande suivante et remplacez-la `12abc34d567e8fa901bc2d34e56789f0` par l'ID du détecteur de votre compte et `us-east-1` par la région dans laquelle vous souhaitez activer la protection RDS.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active automatiquement les deux comptes RDS_LOGIN_EVENTS et RDS_DATA_RISK pour les nouveaux comptes qui rejoignent l'organisation :

```
aws guardduty update-organization-configuration \
  --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
  --region us-east-1 \
  --auto-enable-organization-members NEW \
  --features '[
    {
      "Name": "RDS_LOGIN_EVENTS",
      "AutoEnable": "NEW",
      "AdditionalConfiguration": [
        {
          "Name": "RDS_DATA_RISK",
          "AutoEnable": "NEW"
        }
      ]
    }
  ]'
```

Activez la protection RDS de manière sélective pour les comptes des membres

Choisissez votre méthode d'accès préférée pour activer de manière sélective la surveillance de l'activité de connexion RDS et de l'activité des données RDS pour les comptes des membres.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

Sur la page Comptes, consultez les colonnes Activité de connexion RDS et Activité de données RDS pour connaître l'état de votre compte de membre.

3. Pour activer ou désactiver de manière sélective l'activité de connexion RDS

Sélectionnez le compte pour lequel vous souhaitez configurer la protection RDS. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, choisissez Activité de connexion RDS, puis choisissez l'option appropriée.

4. Pour activer ou désactiver de manière sélective l'activité des données RDS

Sélectionnez le compte pour lequel vous souhaitez configurer la surveillance de l'activité des données RDS. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, choisissez RDS Data Activity, puis choisissez l'option appropriée.

API/CLI

Pour activer ou désactiver la protection RDS de manière sélective pour vos comptes membres, appelez l'opération [updateMemberDetectors](#) d'API en utilisant la vôtre. *detector ID* Passez RDS_DATA_RISK en revue AdditionalConfiguration la RDS_LOGIN_EVENTS fonctionnalité permettant de contrôler indépendamment la surveillance de l'activité des données RDS.

Vous pouvez également utiliser AWS CLI pour activer la protection RDS. Exécutez la commande suivante et remplacez-la *12abc34d567e8fa901bc2d34e56789f0* par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection RDS.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

L'exemple suivant active RDS_LOGIN_EVENTS et RDS_DATA_RISK :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"RDS_LOGIN_EVENTS", "Status": "ENABLED", "AdditionalConfiguration": [{"Name":
"RDS_DATA_RISK", "Status": "ENABLED"}]]'
```

Pour que la surveillance de l'activité de connexion RDS reste activée tout en désactivant la surveillance de l'activité des données RDS, réglez RDS_LOGIN_EVENTS Status sur ENABLED et RDS_DATA_RISK Status sur : DISABLED

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"RDS_LOGIN_EVENTS", "Status": "ENABLED", "AdditionalConfiguration": [{"Name":
"RDS_DATA_RISK", "Status": "DISABLED"}]]'
```

 Note

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activation de la protection RDS pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations ou par le biais d'une invitation, cette section ne s'applique pas à votre compte. Pour plus d'informations, consultez [Activation de la protection RDS dans les environnements à comptes multiples](#).

Après avoir activé la protection RDS, la surveillance des bases [Activité de connexion RDS](#) de données prises en charge dans votre compte GuardDuty commencera.

Choisissez votre méthode d'accès préférée pour configurer la protection RDS pour un compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Sous Protection RDS, choisissez Activer pour activer la protection RDS.
4. Choisissez Enregistrer tout, puis cliquez sur Confirmer et enregistrez.

API/CLI

Exécutez l'opération [updateDetector](#) API en utilisant votre propre identifiant de détecteur régional et en transmettant l'featuresobjet name sous `RDS_LOGIN_EVENTS` et en status tant

que `ENABLED`. Pour activer également la surveillance de l'activité des données RDS, passez `RDS_DATA_RISK` en name dessous `AdditionalConfiguration` avec status défini sur `ENABLED`

Vous pouvez également utiliser AWS CLI pour activer la protection RDS. Exécutez la commande suivante et remplacez-la `12abc34d567e8fa901bc2d34e56789f0` par l'ID du détecteur de votre compte et `us-east-1` par la région dans laquelle vous souhaitez activer la protection RDS.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

L'exemple suivant active `RDS_LOGIN_EVENTS` et `RDS_DATA_RISK` :

```
aws guardduty update-detector \  
  --detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
  --region us-east-1 \  
  --features '[  
    {  
      "Name": "RDS_LOGIN_EVENTS",  
      "Status": "ENABLED",  
      "AdditionalConfiguration": [  
        {  
          "Name": "RDS_DATA_RISK",  
          "Status": "ENABLED"  
        }  
      ]  
    }  
  ]'
```

Résolution des problèmes de surveillance de RDS Protection

GuardDuty RDS Protection analyse et établit le profil de votre activité de connexion RDS pour détecter les menaces d'accès potentielles au [Bases de données prises en charge](#). Pour collecter efficacement les données de télémétrie de sécurité, votre base de données GuardDuty doit être configurée et opérationnelle sans problème. Si votre base de données est mal configurée ou rencontre des problèmes, la surveillance de la sécurité peut être affectée.

La section suivante décrit les problèmes courants et les étapes à suivre pour les résoudre.

Stockage RDS complet

Lorsque votre instance RDS est à court d'espace de stockage, il est possible que la télémétrie de sécurité de GuardDuty soit pas collectée. Atteindre l'allocation de capacité de stockage de l'instance de base de données (`storage-full`) est un état critique, et RDS recommande de résoudre ce problème immédiatement. Pour plus d'informations, consultez la section [Affichage du statut de l'instance](#) dans le guide de l'utilisateur Amazon RDS.

Pour résoudre le `storage-full` statut, vous pouvez effectuer l'une des actions suivantes :

- Activer le dimensionnement automatique du stockage (recommandé) : activez le dimensionnement automatique du stockage Amazon RDS pour gérer automatiquement la capacité de stockage et prévenir les conditions futures. `storage-full` Pour plus d'informations, consultez [la section Gestion automatique de la capacité avec le dimensionnement automatique du stockage Amazon RDS](#) dans le guide de l'utilisateur Amazon RDS.
- Surveillez l'utilisation de votre stockage : vérifiez votre utilisation du stockage à l'aide de l'une des méthodes suivantes :
 - Utilisez CloudWatch les métriques pour afficher les détails du stockage. Pour plus d'informations, consultez [CloudWatch Database Insights](#) dans le guide de CloudWatch l'utilisateur Amazon.
 - Consultez les métriques de stockage en suivant les étapes décrites dans la [section Surveiller les métriques dans une instance Amazon RDS](#) du guide de l'utilisateur Amazon RDS.
- Modifier la capacité de stockage : pour plus d'informations sur l'augmentation de la capacité de stockage de votre instance, consultez la section [Augmenter la capacité de stockage des instances de base](#) de données dans le guide de l'utilisateur Amazon RDS.

Versions non prises en charge sur la base de données principale pour RDS pour PostgreSQL

Les instances de réplication en lecture de RDS pour PostgreSQL nécessitent que l'instance de base de données principale utilise une version de base de données prise en charge et qu'elle soit correctement répliquée à partir de la base de données principale. GuardDuty surveille vos instances uniquement lorsque ces exigences sont satisfaites.

Pour résoudre le problème de version non prise en charge, effectuez l'une des opérations suivantes :

- Vérifiez la compatibilité des versions de base de données : vérifiez que votre base de données RDS pour PostgreSQL principale exécute l'une des versions prises en charge. Pour plus d'informations, consultez [Bases de données prises en charge](#).
- Résolution des problèmes de réplication potentiels : passez en revue et résolvez les problèmes de réplication entre les instances principales et les instances de réplication. Pour plus d'informations à ce sujet, consultez la section [Utilisation des répliques de lecture pour RDS pour PostgreSQL dans le guide de l'utilisateur](#) Amazon RDS.

Considérations supplémentaires en matière de sécurité

Si votre organisation a des exigences de conformité strictes, nous vous recommandons de mettre en œuvre un audit de base de données en plus d'utiliser la protection RDS. Pour plus d'informations sur vos responsabilités en matière de sécurité et le modèle de responsabilité partagée, consultez [la section Sécurité dans Amazon RDS](#) dans le guide de l'utilisateur Amazon RDS.

GuardDuty Protection Lambda

Note

Vous pouvez configurer Lambda Protection ainsi que tous les autres plans de protection à partir d'une seule page de la GuardDuty console. Pour de plus amples informations, veuillez consulter [Configuration des plans de protection](#).

La protection Lambda vous aide à identifier les menaces de sécurité potentielles lorsqu'une fonction [AWS Lambda](#) est invoquée dans votre environnement AWS . Lorsque vous activez la protection Lambda, GuardDuty commence à surveiller les journaux d'activité du réseau Lambda. Cela inclut toutes les fonctions Lambda [Journaux de flux VPC](#) de votre compte (y compris les journaux qui n'utilisent pas le réseau VPC) et les journaux générés lorsque la fonction Lambda est invoquée. Lorsque vous GuardDuty identifiez un trafic réseau suspect indiquant la présence d'un code potentiellement malveillant dans votre fonction Lambda, il en GuardDuty génère un ou plusieurs. [Types de résultat de la protection Lambda](#)

essai gratuit de 30 jours

La liste suivante explique comment fonctionne l'essai gratuit de 30 jours pour votre compte :

- Lorsque vous l'activez GuardDuty Compte AWS dans une nouvelle région pour la première fois, vous bénéficiez d'un essai gratuit de 30 jours. Dans ce cas, la protection Lambda, incluse dans l'essai gratuit, GuardDuty sera également activée.
- Lorsque vous utilisez déjà Lambda Protection GuardDuty et décidez de l'activer pour la première fois, votre compte dans cette région bénéficiera d'un essai gratuit de 30 jours pour Lambda Protection.
- Vous pouvez choisir de désactiver la protection Lambda dans n'importe quelle région à tout moment.
- Au cours de l'essai gratuit de 30 jours, vous pouvez obtenir une estimation de vos coûts d'utilisation pour ce compte et cette région. Après la fin de l'essai gratuit de 30 jours, la protection Lambda n'est pas automatiquement désactivée. Votre compte dans cette région commencera à entraîner des frais d'utilisation. Pour de plus amples informations, veuillez consulter [Surveillance de GuardDuty l'utilisation et estimation des coûts](#).

Les journaux d'activité du réseau Lambda sont sujets à modification, notamment à l'extension à d'autres activités réseau, telles que les données de requête DNS générées par l'appel des fonctions Lambda. L'extension à d'autres formes de surveillance de l'activité réseau augmentera le volume de données à traiter pour la protection Lambda. GuardDuty Cela aura un impact direct sur le coût d'utilisation de la protection Lambda. Chaque fois que vous GuardDuty commencez à surveiller un journal d'activité réseau supplémentaire, il fournit une notification aux comptes qui ont activé la protection Lambda, au moins 30 jours avant la publication.

Note

La surveillance de l'activité du réseau Lambda n'inclut pas les journaux des [fonctions Lambda@Edge](#).

Surveillance de l'activité du réseau Lambda

Lorsque vous activez la protection Lambda, surveille GuardDuty les journaux d'activité du réseau Lambda générés lorsqu'une fonction Lambda associée à votre compte est invoquée. Cela vous permet de détecter les menaces de sécurité potentielles qui pèsent sur la fonction Lambda. Pour les fonctions Lambda configurées pour utiliser le réseau VPC, il n'est pas nécessaire d'activer les journaux de flux VPC pour les interfaces réseau élastiques (ENI) créées par Lambda pour. GuardDuty ne facture que le montant des données des journaux d'activité du réseau Lambda traitées (en Go) pour générer un résultat. GuardDuty optimise les coûts en appliquant des filtres intelligents et en analysant un sous-ensemble de journaux d'activité du réseau Lambda pertinents pour la détection des menaces.

GuardDuty ne gère pas les journaux d'activité de votre réseau Lambda (y compris les journaux de flux VPC et non VPC) et ne les rend pas accessibles dans votre compte.

Activation de la protection Lambda dans les environnements à comptes multiples

Dans un environnement multi-comptes, seul le compte d' GuardDuty administrateur délégué a la possibilité d'activer ou de désactiver la protection Lambda pour les comptes des membres de son organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration depuis leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes des membres à l'aide de AWS Organizations. Le compte GuardDuty administrateur délégué peut choisir d'activer

automatiquement la surveillance de l'activité réseau Lambda pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements à comptes multiples, consultez [Gérer plusieurs comptes sur Amazon](#). GuardDuty

Activation de la protection Lambda pour le compte administrateur délégué GuardDuty

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance de l'activité réseau Lambda pour le compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sous Paramètres, choisissez Protection Lambda.
3. Sur la page Protection Lambda, choisissez Modifier.
4. Effectuez l'une des actions suivantes :

Utilisation d'Activer pour tous les comptes

- Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
- Choisissez Enregistrer.

Utilisation de Configurer les comptes manuellement

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Choisissez Enregistrer.

API/CLI

Exécutez l'opération [updateDetector](#) API en utilisant votre propre identifiant de détecteur régional et en transmettant l'featuresobjet name sous LAMBDA_NETWORK_LOGS et en status tant queENABLED.

Vous pouvez également l'utiliser AWS CLI pour activer la protection Lambda. Exécutez la commande suivante et remplacez-la `12abc34d567e8fa901bc2d34e56789f0` par l'ID du

détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection Lambda.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Auto-enable Surveillance de l'activité du réseau Lambda pour tous les comptes membres

Choisissez votre méthode d'accès préférée pour activer la fonctionnalité Surveillance de l'activité du réseau Lambda pour tous les comptes membres. Cela inclut les comptes membres existants et les nouveaux comptes qui rejoignent l'organisation.

Console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

Utilisation de la page Plans de protection

1. Dans le volet de navigation, sélectionnez Plans de protection.
2. Choisissez Configurer toutes les activations.
3. Sous Lambda Protection, sélectionnez Activer pour tous les comptes. Cette action active automatiquement la surveillance de l'activité du réseau Lambda pour les comptes existants et nouveaux de l'organisation.
4. Choisissez Enregistrer tout, puis cliquez sur Confirmer et enregistrez.

 Note

La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez Auto-enable les préférences avant Ajouter des comptes sur invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous Surveillance de l'activité du réseau Lambda.

 Note

Par défaut, cette action active automatiquement l'option Auto-enable GuardDuty pour les nouveaux comptes membres.

4. Choisissez Enregistrer.

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter [Activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres](#).

API/CLI

Pour activer ou désactiver de manière sélective la surveillance de l'activité réseau Lambda pour vos comptes membres, appelez l'opération d'[updateMemberDetectors](#) API en utilisant la vôtre. *detector ID*

Vous pouvez également l'utiliser AWS CLI pour activer la protection Lambda. Exécutez la commande suivante et remplacez-la *12abc34d567e8fa901bc2d34e56789f0* par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection Lambda.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --region us-east-1--features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer la surveillance de l'activité du réseau Lambda pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la surveillance de l'activité du réseau Lambda pour tous les comptes membres actifs existants de l'organisation.

Console

Pour configurer la surveillance de l'activité du réseau Lambda pour tous les comptes membres actifs existants

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.

Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, sélectionnez Plans de protection.
3. Choisissez Configurer toutes les activations. Sous Lambda Protection, vous pouvez consulter l'état actuel de la configuration. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Confirmer.

API/CLI

Pour activer ou désactiver de manière sélective la surveillance de l'activité réseau Lambda pour vos comptes membres, appelez l'opération d'[updateMemberDetectors](#) API en utilisant la vôtre.

detector ID

Vous pouvez également l'utiliser AWS CLI pour activer la protection Lambda. Exécutez la commande suivante et remplacez-la *12abc34d567e8fa901bc2d34e56789f0* par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection Lambda.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features ' [{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"} ] '
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Auto-enable Surveillance de l'activité du réseau Lambda pour les nouveaux comptes membres

Choisissez votre méthode d'accès préférée pour activer la surveillance de l'activité du réseau Lambda pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte d' GuardDuty administrateur délégué peut activer la surveillance de l'activité réseau Lambda pour les nouveaux comptes membres d'une organisation, à l'aide de la page Lambda Protection ou des comptes.

Pour activer automatiquement la surveillance de l'activité du réseau Lambda pour les nouveaux comptes membres

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l'une des actions suivantes :

- À l'aide de la page Plans de protection :
 1. Dans le volet de navigation, sélectionnez Plans de protection.
 2. Choisissez Configurer toutes les activations.
 3. Choisissez Configurer les comptes manuellement.
 4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la protection Lambda sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
 5. Choisissez Enregistrer.
- Utilisation de la page Comptes :
 1. Dans le panneau de navigation, choisissez Accounts (Comptes).
 2. Sur la page Comptes, sélectionnez Auto-enablePréférences.
 3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous Surveillance de l'activité du réseau Lambda.
 4. Choisissez Enregistrer.

API/CLI

Pour activer la surveillance de l'activité réseau Lambda pour les nouveaux comptes membres, appelez l'opération d'[UpdateOrganizationConfiguration](#)API en utilisant la vôtre. *detector ID*

Vous pouvez également l'utiliser AWS CLI pour activer la protection Lambda. L'exemple suivant montre comment activer la surveillance de l'activité du réseau Lambda pour un seul compte membre. *12abc34d567e8fa901bc2d34e56789f0* Remplacez-le par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection Lambda. Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes qui rejoignent l'organisation, définissez `AutoEnable` sur `NONE`.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le volet de navigation, sous Settings, choisissez Accounts.

Sur la page Comptes, examinez la colonne Surveillance de l'activité du réseau Lambda. Elle indique si la surveillance de l'activité du réseau Lambda est activée ou non.

3. Sélectionnez le compte pour lequel vous souhaitez configurer la protection Lambda. Vous pouvez choisir plusieurs comptes à la fois.
4. Dans le menu déroulant Modifier les plans de protection, choisissez Surveillance de l'activité du réseau Lambda, puis choisissez une action appropriée.

API/CLI

Appelez l'[updateMemberDetectors](#) API en utilisant la vôtre *detector ID*.

Vous pouvez également l'utiliser AWS CLI pour activer la protection Lambda.

12abc34d567e8fa901bc2d34e56789f0 Remplacez-le par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection Lambda.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de UnprocessedAccounts. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activation de la protection Lambda pour un compte autonome

Un compte autonome prend la décision d'activer ou de désactiver un plan de protection Compte AWS dans un espace spécifique Région AWS.

Si votre compte est associé à un compte GuardDuty administrateur par le biais AWS Organizations d'une invitation ou par le biais d'une invitation, cette section ne s'applique pas à votre compte.

Pour de plus amples informations, veuillez consulter [Activation de la protection Lambda dans les environnements à comptes multiples](#).

Une fois que vous aurez activé la protection Lambda, la surveillance GuardDuty commencera [Surveillance de l'activité du réseau Lambda](#) dans votre compte.

Choisissez votre méthode d'accès préférée pour configurer la protection Lambda pour un compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sous Paramètres, choisissez Protection Lambda.
3. La page Protection Lambda indique l'état actuel de votre compte. Choisissez Activer pour activer la protection Lambda dans votre compte.
4. Choisissez Confirmer pour enregistrer votre sélection.

API/CLI

Exécutez l'opération [updateDetector](#) API en utilisant votre propre identifiant de détecteur régional et en transmettant l'featuresobjet name sous LAMBDA_NETWORK_LOGS et en status tant queENABLED.

Vous pouvez également l'utiliser AWS CLI pour activer la protection Lambda. Exécutez la commande suivante et remplacez-la *12abc34d567e8fa901bc2d34e56789f0* par l'ID du détecteur de votre compte et *us-east-1* par la région dans laquelle vous souhaitez activer la protection Lambda.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" :
"ENABLED"}]'
```


GuardDuty Enquête (aperçu)

GuardDuty Investigation fournit une analyse de AI-powered sécurité de vos GuardDuty résultats et de vos comptes. Lorsque vous créez une enquête, GuardDuty examinez le contexte, les activités connexes des 90 derniers jours, les ressources concernées, les renseignements sur les menaces et les indicateurs de menace à l'aide de graphiques de connaissances. Chaque enquête fournit une évaluation de l'élimination des menaces avec un score de confiance, une classification selon la technique MITRE ATT&CK®, des preuves à l'appui et des recommandations exploitables.

Chaque enquête produit les informations suivantes :

- Niveau de risque : évaluation du risque global : info, faible, moyen, élevé ou critique.
- Confiance : niveau de confiance de l'évaluation : inconnu, faible, moyen ou élevé.
- Résumé — Description des résultats de l'enquête et des principales observations.
- Détails de l'enquête — Informations supplémentaires et contexte liés à l'enquête.
- Actions recommandées : actions détaillées, y compris les commandes de l'interface de ligne de commande, que vous pouvez effectuer pour résoudre les problèmes identifiés.

Note

GuardDuty Investigation n'est disponible que dans les 10 AWS régions commerciales suivantes : USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), Canada (Centre), Europe (Francfort), Europe (Irlande), Europe (Londres), Europe (Paris), Europe (Stockholm) et Asie-Pacifique (Tokyo).

Types d'analyses

GuardDuty L'investigation soutient les trois types d'analyse suivants :

- Analyse des résultats : analyse des GuardDuty résultats spécifiques lorsque vous spécifiez l'ID du résultat (32 caractères hexadécimaux). Pour la version préliminaire, GuardDuty Investigation prend en charge tous les résultats de la détection étendue des menaces (XTD) et certains résultats des plans de base, S3 et Runtime.
- Analyse du compte : analyse la position de menace d'un AWS compte lorsque vous fournissez un identifiant de AWS compte à 12 chiffres.

- **Analyse de l'organisation** : analyse la position de votre organisation face aux menaces.

Cross-Region inférence

GuardDuty L'investigation s'appuie sur le service d' Cross-Region inférence (CRIS), qui sélectionne automatiquement la solution optimale Région AWS dans votre zone géographique pour traiter l'analyse de l'enquête et générer le rapport d'enquête. Cela maximise les ressources de calcul disponibles, la disponibilité des modèles et offre la meilleure expérience client.

Vos données restent stockées uniquement dans la région d'où provient la demande d'enquête. Toutefois, les données d'enquête et les résultats récapitulatifs peuvent être traités en dehors de cette région. Toutes les données sont transmises de manière cryptée sur le réseau sécurisé Amazon.

GuardDuty Investigation achemine en toute sécurité vos demandes d'inférence vers les ressources de calcul disponibles dans la zone géographique d'origine de la demande, comme indiqué dans le tableau suivant.

Cross-Region routage par inférence

Zone géographique prise en charge	GuardDuty Région	Régions d'inférence
États-Unis	USA Est (Virginie du Nord)	USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon)
États-Unis	USA Est (Ohio)	USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon)
États-Unis	USA Ouest (Oregon)	USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon)
États-Unis	Canada (Centre)	Canada (centre), États-Unis est (Virginie du Nord), États-Unis est (Ohio), États-Unis ouest (Oregon)
Europe	Europe (Francfort)	Europe (Francfort), Europe (Stockholm), Europe (Milan), Europe (Espagne), Europe (Irlande), Europe (Paris)

Zone géographique prise en charge	GuardDuty Région	Régions d'inférence
Europe	Europe (Irlande)	Europe (Francfort), Europe (Stockholm), Europe (Milan), Europe (Espagne), Europe (Irlande), Europe (Paris)
Europe	Europe (Londres)	Europe (Francfort), Europe (Stockholm), Europe (Milan), Europe (Espagne), Europe (Irlande), Europe (Londres), Europe (Paris)
Europe	Europe (Paris)	Europe (Francfort), Europe (Stockholm), Europe (Milan), Europe (Espagne), Europe (Irlande), Europe (Paris)
Europe	Europe (Stockholm)	Europe (Francfort), Europe (Stockholm), Europe (Milan), Europe (Espagne), Europe (Irlande), Europe (Paris)
Japon	Asie-Pacifique (Tokyo)	Asie-Pacifique (Tokyo), Asie-Pacifique (Osaka)

Conditions préalables

Avant de pouvoir utiliser GuardDuty Investigation, assurez-vous que les conditions suivantes sont remplies :

- Vous devez disposer d'un GuardDuty détecteur actif à l' Région AWS endroit où vous souhaitez créer des enquêtes. Pour plus d'informations sur l'activation GuardDuty, consultez [Commencer avec GuardDuty](#).
- Vous devez activer la fonction GuardDuty Investigation sur votre détecteur.

Console

1. Ouvrez la GuardDuty console.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Investigations alimentées par l'IA - Aperçu, choisissez Activer.

API/CLI

Appelez l'[UpdateDetector](#) API et activez la AI_ANALYST fonction sur votre détecteur.

```
aws guardduty update-detector \  
  --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \  
  --features '[{"Name": "AI_ANALYST", "Status": "ENABLED"}]'
```

- Votre identité IAM doit disposer des autorisations requises pour effectuer des actions d'investigation. Les actions IAM suivantes sont requises :
 - guardduty:CreateInvestigation— Nécessaire pour créer une nouvelle enquête.
 - guardduty:GetInvestigation— Nécessaire pour récupérer les résultats de l'enquête.
 - guardduty:ListInvestigations— Obligatoire pour répertorier les investigations relatives à un détecteur.

L'exemple de politique IAM suivant autorise l'utilisation de toutes les actions GuardDuty d'investigation :

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "guardduty:CreateInvestigation",  
        "guardduty:GetInvestigation",  
        "guardduty:ListInvestigations"  
      ],  
      "Resource": "arn:aws:guardduty:us-west-2:123456789012:detector/2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7"  
    }  
  ]  
}
```

Modèle d'accès pour les comptes d'administrateur et de membre

Les règles d'accès suivantes s'appliquent à GuardDuty Investigation selon que vous utilisez un compte administrateur ou un compte membre :

- **Comptes d'administrateur** : peuvent créer, obtenir et répertorier des enquêtes pour eux-mêmes et leurs comptes membres.
- **Comptes des membres** : ils ne peuvent obtenir et répertorier les enquêtes que pour leur propre compte. Les comptes membres ne peuvent pas créer d'enquêtes et ne peuvent pas accéder aux enquêtes appartenant à d'autres comptes ou au compte administrateur.

Création d'une enquête

Vous pouvez créer une enquête pour analyser les GuardDuty résultats et les comptes dans votre AWS environnement. L'enquête s'exécute de manière asynchrone en arrière-plan. Après avoir créé une enquête, utilisez l'ID de l'enquête pour vérifier son statut et récupérer les résultats.

Important

Pendant la prévisualisation, vous pouvez lancer jusqu'à 10 enquêtes par compte et par jour, avec une limite totale de 100 enquêtes par compte. Les enquêtes échouées ne sont pas prises en compte dans ces quotas. Si vous utilisez le API/CLI, l'invite de déclenchement peut contenir jusqu'à 2 048 caractères.

Choisissez votre méthode d'accès préférée pour créer une enquête.

Console

1. Ouvrez la GuardDuty console et accédez à **Investigations** dans la barre de navigation de gauche.
2. Choisissez **Initier une enquête**.
3. Sélectionnez un champ d'investigation :
 - **Un résultat spécifique** — Entrez l'identifiant du résultat que vous souhaitez analyser.
 - **Mon compte** (version autonome uniquement) — Aucune saisie supplémentaire n'est requise. GuardDuty analysera votre compte.
 - **Un compte spécifique** (administrateur uniquement) — Entrez l'identifiant de AWS compte à 12 chiffres.
 - **Tous les comptes de l'organisation** (administrateur uniquement) — Aucune saisie supplémentaire n'est requise.

4. Choisissez Initier une enquête pour démarrer l'analyse.

API/CLI

Exécutez l'opération d>CreateInvestigationAPI pour démarrer une nouvelle enquête. Vous devez fournir l'identifiant du détecteur et une invite de déclenchement décrivant les éléments à examiner.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty create-investigation \
  --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
  --trigger-prompt "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
account 123456789012"
```

Dans la commande précédente, remplacez le *detector-id* par votre propre identifiant de détecteur et *trigger-prompt* par une description de ce que vous souhaitez étudier.

Vous pouvez éventuellement inclure un `--client-token` paramètre pour l'idempotence. Si vous réessayez la demande avec le même jeton client, GuardDuty renvoie l'enquête existante au lieu de créer un doublon.

Exemple de sortie :

```
{
  "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890"
}
```

Exigences relatives au déclenchement rapide

L'invite de déclenchement doit décrire les éléments à examiner. GuardDuty détermine le type d'analyse en fonction du contenu de votre invite :

- Analyse des résultats — Incluez exactement un identifiant de recherche (chaîne hexadécimale de 32 caractères) dans l'invite. La découverte doit exister et appartenir au compte de l'appelant ou à un compte de membre. Vous ne pouvez pas inclure plusieurs identifiants de recherche dans une seule invite.

- **Analyse du compte** — Incluez exactement un identifiant de AWS compte à 12 chiffres dans l'invite. L'appelant doit être l'administrateur de ce compte. Vous ne pouvez pas inclure plusieurs identifiants de compte dans une seule invite.
- **Analyse de l'organisation** : décrivez un problème de sécurité à l'échelle de l'organisation dans votre invite. L'enquête analyse les signaux dans l'ensemble de l'organisation.

GuardDuty utilise l'IA pour interpréter votre invite de forme libre et déterminer la portée d'analyse appropriée. Si vous incluez un identifiant de recherche, il effectue une analyse de recherche. Si vous incluez un identifiant de compte, il effectue une analyse du compte. Si votre invite décrit un problème à l'échelle de l'organisation, elle effectue une analyse de l'organisation. Si l'invite ne correspond pas à un type d'analyse spécifique, l'enquête analyse par défaut le compte de l'appelant.

Voici des exemples de messages de déclenchement pour chaque type d'analyse :

- **Analyse des résultats** — "Investigate finding
1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in account 123456789012"
- **Analyse des comptes** — "Analyze findings in account with id 123456789012"
- **Analyse de l'organisation** — "Analyze findings in my organization"

Création d'une enquête pour un compte membre

Si vous êtes un compte administrateur, vous pouvez créer une enquête pour un compte membre en incluant l'identifiant du compte membre dans l'invite de déclenchement. Utilisez l'ID de détecteur du compte administrateur dans la commande. Les résultats de l'enquête contiendront les résultats du compte membre spécifié.

```
aws guardduty create-investigation \  
  --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \  
  --trigger-prompt "Analyze findings in account with id 111122223333"
```

Dans la commande précédente, remplacez le **detector-id** par l'ID de détecteur de votre compte administrateur. L'identifiant de compte à 12 chiffres figurant dans l'invite de déclenchement identifie le compte du membre à examiner.

Affichage des résultats de l'enquête

Après avoir créé une enquête, vous pouvez récupérer les résultats, y compris le résumé, les détails de l'enquête, le niveau de confiance et la recommandation. Une enquête peut avoir l'un des statuts suivants :

- **EN COURS** — L'enquête est toujours en cours.
- **TERMINÉ** — L'enquête s'est terminée avec succès et les résultats sont disponibles.
- **ÉCHEC** — L'enquête a détecté une erreur. Consultez le champ d'erreur pour plus de détails.

Choisissez votre méthode d'accès préférée pour consulter les résultats de l'enquête.

AI-generated les analyses et les recommandations peuvent contenir des erreurs ou des évaluations incomplètes. Un examen humain est recommandé.

Console

1. Ouvrez la GuardDuty console et accédez à **Investigations** dans la barre de navigation de gauche.
2. Dans le tableau des enquêtes, recherchez l'enquête terminée que vous souhaitez consulter.
3. Cliquez sur le lien du titre de l'enquête pour ouvrir la page de détails.

Note

Les titres des enquêtes ne sont cliquables que lorsque le statut est Terminé.

API/CLI

Exécutez l'opération d'GetInvestigationAPI pour récupérer tous les détails d'une enquête terminée.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty get-investigation \
```



```
--detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
--investigation-id a1b2c3d4-5678-90ab-cdef-ef1234567890
```

Exemple de résultat pour une enquête terminée :

```
{
  "Investigation": {
    "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
    "Status": "COMPLETED",
    "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
account 123456789012",
    "TriggeredBy": "123456789012",
    "RiskLevel": "Critical",
    "Risk": "Detection logic is valid but no live resources are compromised.",
    "Confidence": "High",
    "Summary": "{\\"keyObservations\\":{\\"title\\":\\"...\\",\\"narrative\\":\\"...\\",
\\"observations\\":[...]},\\"countermeasures\\":[...],\\"threatAssessment\\":{...}}",
    "Cloud": {
      "Provider": "AWS",
      "Region": "us-east-1",
      "Account": "123456789012"
    },
    "Metadata": {
      "Product": {
        "Name": "Amazon GuardDuty AI Analyst",
        "Feature": "Investigation"
      },
      "Version": "1.0.0"
    },
    "StartTime": 1705319400.0,
    "EndTime": 1705319700.0
  }
}
```

Le Summary champ contient une chaîne JSON contenant les résultats complets de l'enquête, y compris les principales observations, les contre-mesures à l'aide de commandes CLI et une évaluation des menaces MITRE ATT&CK®.

Interpréter les résultats des enquêtes

Le tableau suivant décrit les niveaux de risque qu'une enquête peut révéler :

Niveaux de risque liés aux enquêtes

Niveau de risque	Description
Info (Infos)	Résultat informatif sans risque identifié pour l'environnement.
Faible	Risque mineur qui ne nécessitera probablement pas une action immédiate.
Moyenne	Risque modéré que vous devez examiner et qui pourrait nécessiter des mesures correctives.
Élevée	Risque important nécessitant une enquête et une correction rapides.
Critique	Risque grave nécessitant une action immédiate pour éviter tout nouveau compromis.

Le tableau suivant décrit les niveaux de confiance :

Niveaux de confiance dans les enquêtes

Niveau de confiance	Description
Je ne sais pas	Les données sont insuffisantes pour déterminer la confiance dans l'évaluation.
Faible	Des preuves limitées étayent cette évaluation.
Moyenne	Des preuves modérées étayent cette évaluation.
Élevée	Des preuves solides étayent cette évaluation.

Enquêtes sur les listes

Vous pouvez répertorier toutes les enquêtes relatives à un détecteur, avec un tri et une pagination facultatifs. Cela vous permet d'examiner et de suivre l'état de plusieurs enquêtes.

Choisissez votre méthode d'accès préférée pour répertorier les enquêtes.

Console

1. Ouvrez la GuardDuty console et accédez à **Investigations** dans la barre de navigation de gauche.
2. Le tableau des enquêtes affiche toutes les enquêtes pour le détecteur actuel avec leur statut, leur niveau de risque et leur horodatage.

API/CLI

Exécutez l'opération `ListInvestigations` API pour répertorier les résumés d'enquêtes pour un détecteur.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page **Paramètres** de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

```
aws guardduty list-investigations \  
  --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \  
  --max-results 10
```

Vous pouvez trier les résultats en spécifiant un `--sort-criteria` paramètre. L'exemple suivant répertorie les enquêtes triées par heure de début dans l'ordre décroissant :

```
aws guardduty list-investigations \  
  --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \  
  --sort-criteria '{"attributeName": "START_TIME", "orderBy": "DESC"}' \  
  --max-results 10
```

Les attributs de tri disponibles sont `START_TIME`, `END_TIME`, `STATUS`, `RISK_LEVEL`, et `CONFIDENCE`. Vous pouvez trier par ordre `ASC` (croissant) ou `DESC` (décroissant).

Exemple de sortie :

```
{  
  "Investigations": [  
    {  
      "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",  
      "Status": "COMPLETED",  
      "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6  
in account 123456789012",
```

```
    "RiskLevel": "Critical",
    "Confidence": "High",
    "StartTime": 1705319400.0,
    "EndTime": 1705319700.0,
    "AccountId": "123456789012"
  },
  {
    "InvestigationId": "b2c3d4e5-6789-01bc-def0-ef2345678901",
    "Status": "COMPLETED",
    "TriggerPrompt": "Analyze findings in account with id 123456789012",
    "RiskLevel": "High",
    "Confidence": "High",
    "StartTime": 1705315800.0,
    "EndTime": 1705316100.0,
    "AccountId": "123456789012"
  },
  {
    "InvestigationId": "c3d4e5f6-7890-12cd-ef01-ef3456789012",
    "Status": "COMPLETED",
    "TriggerPrompt": "Analyze findings in my organization",
    "RiskLevel": "Medium",
    "Confidence": "Medium",
    "StartTime": 1705312200.0,
    "EndTime": 1705312500.0,
    "AccountId": "123456789012"
  }
]
```

Si la réponse inclut une `NextToken` valeur, transmettez-la dans une requête ultérieure pour récupérer la page de résultats suivante. Vous pouvez récupérer jusqu'à 50 résultats par page.

Règles de détection personnalisées dans GuardDuty

Les règles de détection personnalisées fournissent une bibliothèque de règles prédéfinies qui détectent les activités auxquelles vous ne vous attendez pas dans votre AWS environnement. GuardDuty élabore et gère ces règles et décrit chacune d'entre elles en utilisant le vocabulaire des techniques de menace établi, tiré de catalogues tels que MITRE ATT&CK® et le catalogue des techniques de AWS menace. Vous activez chaque règle pour l'activité que vous souhaitez détecter, soit en mode de fonctionnement à sec pour la mesurer en premier, soit en mode réel pour générer des résultats.

Les équipes de sécurité savent souvent que certaines actions ne doivent pas être effectuées sur des comptes spécifiques. Une action telle que le partage d'une AMI, la suppression des journaux de flux VPC ou la connexion sans MFA peut être routinière dans un compte et être un signe de compromission dans un autre. La plupart des GuardDuty résultats identifient des activités suspectes dans n'importe quel environnement. Les règles de détection personnalisées vous permettent de détecter les activités suspectes uniquement dans les comptes pour lesquels vous ne vous y attendez pas.

Les règles de détection personnalisées utilisent les concepts suivants :

Règle

Une détection prédéfinie que GuardDuty possède et gère. Chaque règle cible une technique de menace et définit les conditions qui la font correspondre.

Association

Le lien entre une règle et un compte. Une association enregistre le mode d'exécution de la règle pour ce compte. Une règle sans association n'est pas évaluée.

Mode

Comportement d'une règle associée lorsqu'elle correspond à une activité. Chaque règle prend en charge deux modes :

- En direct : GuardDuty génère un résultat lorsque la règle correspond à l'activité. Le mode Live n'expire pas.
- Exécution à sec : GuardDuty évalue la règle et émet des CloudWatch métriques Amazon mais ne génère pas de résultats. Utilisez le test à sec pour mesurer le volume du signal avant de procéder à une détection en direct. GuardDuty émet ces mesures uniquement lorsque la règle

correspond à un événement, de sorte qu'une règle qui ne correspond jamais ne produit aucune métrique de course à sec. Le cycle à sec expire automatiquement au bout de 14 jours.

Configuration de l'organisation

Configuration de règles que le compte d' GuardDuty administrateur délégué applique aux comptes des membres d'une organisation. GuardDuty crée les associations individuelles dans chaque compte ciblé, y compris les comptes qui se joignent ultérieurement. Pour plus d'informations, consultez [Gestion des règles de détection personnalisées dans les environnements à comptes multiples](#).

Signal

Une occurrence observée de l'activité détectée par une règle. GuardDuty agrège les signaux connexes en une seule constatation. Pour plus d'informations, consultez [Trouver une agrégation](#).

Rubriques

- [Comment fonctionnent les règles de détection personnalisées](#)
- [Règles de détection personnalisées disponibles](#)
- [Gestion des règles de détection personnalisées](#)
- [Gestion des règles de détection personnalisées dans les environnements à comptes multiples](#)

Comment fonctionnent les règles de détection personnalisées

Commencez par parcourir les règles que GuardDuty propose d'identifier celles qui détectent les activités pertinentes pour votre environnement. Associez ensuite chaque règle aux comptes où l'activité est inattendue. Pour plus d'informations sur l'association de règles à des comptes, consultez [Gestion des règles de détection personnalisées](#).

Sources de données et signaux

Après avoir associé une règle, GuardDuty surveille les sources de données dont dépend la règle et évalue les journaux entrants pour détecter les événements correspondants. Les règles de détection personnalisées prennent en charge les événements AWS CloudTrail de gestion et les événements de surveillance du temps d'exécution. Lorsque l'activité observée correspond à une règle, GuardDuty génère un signal. Un signal représente une seule occurrence observée de l'activité détectée par la règle.

Chaque source de données a ses propres exigences :

AWS CloudTrail événements de gestion

GuardDuty analyse ces événements dans chaque compte où il GuardDuty est activé. Aucune configuration supplémentaire n'est requise.

Événements de surveillance du temps d'exécution

Les règles de surveillance de l'exécution évaluent l'activité des processus, des fichiers et du réseau que l'agent de GuardDuty sécurité observe sur vos ressources. Une règle de surveillance du temps d'exécution ne peut correspondre à l'activité que sur une ressource qui répond aux deux exigences suivantes :

- La surveillance du temps d'exécution est activée pour le type de ressource : Amazon EKS, Amazon EC2 ou Amazon ECS on Fargate. Pour plus d'informations, consultez [GuardDuty Surveillance du temps d'exécution](#).
- L'agent GuardDuty de sécurité s'exécute sur la ressource, à une version d'agent égale ou supérieure à la version minimale de la règle pour cette plate-forme.

Chaque règle de surveillance du temps d'exécution indique la version minimale de l'agent requise sur chaque plate-forme sur laquelle elle peut être exécutée. Pour consulter ces exigences, appelez l'[GetCustomDetectionRule](#)opération.

Si l'agent d'une ressource est plus ancien que la version minimale d'une règle, la règle ne correspond pas à l'activité sur cette ressource. GuardDuty ne signale pas d'erreur dans ce cas, alors tenez l'agent informé des ressources sur lesquelles vous activez les règles de surveillance du temps d'exécution. Pour plus d'informations sur les versions des agents, consultez [GuardDuty versions publiées de l'agent de sécurité](#).

Modes

Chaque association fonctionne selon l'un des deux modes suivants :

- En direct : GuardDuty génère un résultat lorsque la règle correspond.
- Run à sec : GuardDuty émet CloudWatch des indicateurs Amazon qui comptabilisent la fréquence à laquelle la règle correspond, mais ne génèrent pas de résultats. Utilisez l'essai à sec pour mesurer la fréquence à laquelle une règle correspond avant qu'elle ne puisse créer des résultats ou déclencher des réponses automatisées. Les associations gérées à sec expirent 14 jours après leur création, les associations actives n'expirent pas.

Pour plus d'informations, consultez [Course à sec](#) et [Direct](#).

Trouver une agrégation

Chaque résultat suit le format `Tactic:Service/Technique`, par exemple, `Persistence:IAM/AccountManipulation` ou `Persistence:Runtime/SuspiciousCommand`. La manière dont GuardDuty les signaux sont regroupés dans les résultats dépend de la source de données qui a généré le signal, comme décrit dans la liste suivante :

- **AWS CloudTrail règles** : GuardDuty regroupe les signaux qui partagent la même tactique, le même service et la même technique en un seul résultat. Un seul résultat peut contenir plusieurs signaux lorsqu'on GuardDuty observe la même activité à plusieurs reprises à partir du même principe.
- **Règles de surveillance du temps d'exécution** : GuardDuty regroupe les signaux qui partagent les mêmes règles, ressources et détails de processus en une seule constatation. Chaque découverte couvre une ressource, telle qu'une instance, une tâche ou un conteneur. Les détails du processus de GuardDuty comparaison dépendent du type de recherche. Par exemple, les résultats de modification de fichier comparent également l'opération sur le fichier et l'utilisateur qui a exécuté le processus. Une correspondance répétée met à jour le résultat existant au lieu d'en créer un nouveau. Les résultats des différentes règles restent séparés, même lorsque les règles génèrent le même type de recherche pour la même ressource et le même processus.

Pour plus d'informations sur la structure de recherche et les champs, consultez [Règles de détection personnalisées pour trouver des détails](#).

Champs d'événements expurgés

évaluent les champs qui AWS CloudTrail enregistrent un événement. AWS CloudTrail La rédaction a lieu en amont de. GuardDuty Un AWS service peut supprimer la valeur d'un champ dans les événements qu'il publie. Cette rédaction protège les données potentiellement sensibles. Lorsqu'un champ est expurgé, AWS CloudTrail enregistre que le champ était présent mais n'enregistre pas sa valeur.

Le service qui publie l'événement décide des champs à supprimer. Un service expédie un champ lorsque celui-ci peut contenir des informations sensibles. La rédaction s'applique au champ, et non à une valeur spécifique. Un service expédie donc un champ même lorsque la valeur d'une demande particulière n'est pas sensible. Il expédie ces champs pour chaque demande, que vous utilisiez la Console de gestion AWS AWS CLI ou un AWS SDK.

GuardDuty Impossible d'évaluer une valeur qui ne figure pas dans l'événement. Si la logique de détection d'une règle dépend d'un champ expurgé, la règle ne correspond pas. GuardDuty ne produit alors aucun signal ni aucune constatation, même si l'activité s'est produite. Une règle n'est pas affectée si elle inspecte uniquement les champs que les services ne suppriment pas, tels que le nom de l'événement, le AWS service et l'identité de l'appelant.

La rédaction peut également faire correspondre une règle à une demande mais pas à une autre ayant le même effet. Lorsqu'une opération d'API accepte plusieurs champs pour la même modification, un champ peut être expurgé et un autre non. La correspondance de la règle dépend alors du champ utilisé par la demande.

Note

Les règles de détection personnalisées constituent une fonctionnalité de détection et non un enregistrement d'audit complet. Pour vérifier si un appel d'API spécifique s'est produit dans votre compte, passez en revue l'événement dans AWS CloudTrail. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des AWS CloudTrail événements](#).

Règles de détection personnalisées disponibles

Les règles de détection personnalisées étendent la détection des menaces qu' GuardDuty elle fournit. GuardDuty propose une bibliothèque de règles d'adhésion que vous pouvez choisir d'activer en fonction des risques spécifiques à votre environnement. Pour obtenir la liste actuelle des règles disponibles, utilisez l'opération [ListCustomDetectionRules](#)API. Pour les types de recherche générés par chaque règle, consultez [Règles de détection personnalisées : types de recherche](#).

Note

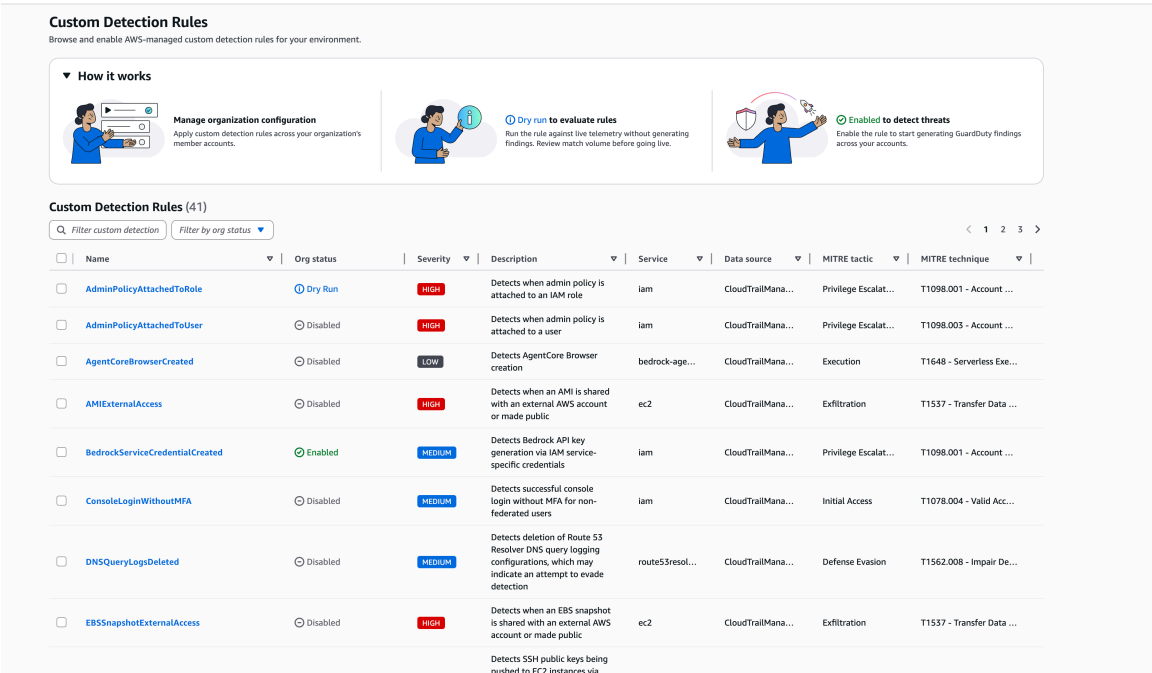
La disponibilité des règles individuelles dépend de la disponibilité du AWS service et de la fonctionnalité correspondants dans chaque région. Par exemple, les règles qui ciblent AWS les Organizations ou Amazon Simple Email Service ne sont disponibles que dans les régions où ces services sont disponibles. De même, les règles qui ciblent les URL des fonctions Lambda ou les instances de SageMaker blocs-notes AI ne sont disponibles que dans les régions où ces fonctionnalités sont prises en charge.

Afficher la logique de détection des règles

Chaque règle définit des conditions spécifiques qui déterminent le moment où elle se déclenche. Vous pouvez inspecter la logique de détection de n'importe quelle règle :

- Console : dans la GuardDuty console, accédez à Règles de détection personnalisées et choisissez un nom de règle. Le panneau divisé affiche la logique de détection de la règle dans l'onglet Détails.
- API — Appelez l'[GetCustomDetectionRule](#) opération. La réponse inclut l'expression de la règle dans le `Definition.Expression` champ.

L'image suivante montre le catalogue de règles de détection personnalisées.



L'image suivante montre le panneau de détails des règles avec la logique de détection.

DNSQueryLogsDeleted

Detects deletion of Route 53 Resolver DNS query logging configurations, which may indicate an attempt to evade detection

Actions

Status	Enabled	
Service	route53resolver	
Severity	MEDIUM	
Data source	CloudTrailManagementEvent	
Language	SQL	
Schema	CloudTrail	
MITRE tactic	Defense Evasion	
MITRE technique	T1562.008 - Impair Defenses: Disable Cloud Logs	
Last updated	June 12, 2026, 16:26:17 (UTC-07:00)	
Created	May 14, 2026, 11:26:00 (UTC-07:00)	

Details

Metrics

Detection logic

1 eventSource = 'route53resolver.amazonaws.com'

2 AND eventName = 'DeleteResolverQueryLogConfig'

3 AND errorCode IS NULL

Fonctions utilisées dans la logique de détection

Les règles de détection personnalisées utilisent des conditions SQL. AWS CloudTrail les règles évaluent les champs d' AWS CloudTrail événements, et certaines utilisent des fonctions spécialisées pour inspecter les structures JSON imbriquées dans les champs d'événements, telles que `requestParameters` et `responseElements`. Les règles de surveillance de l'exécution évaluent les champs des événements d'exécution, et nombre d'entre elles utilisent des fonctions d'expression régulière, principalement pour faire correspondre les lignes de commande des processus. Le tableau suivant décrit les fonctions susceptibles d'apparaître dans la logique de détection des règles.

Une règle inspectant un champ imbriqué dépend de la présence de ce champ dans l'événement. Pour plus d'informations sur les champs que AWS CloudTrail n'enregistrent pas, consultez [Champs d'événements expurgés](#).

Fonction	Renvoie	Description
<code>get_json_object(json, path)</code>	Chaîne	Extrait une valeur d'un document JSON à l'aide d'un chemin séparé par des points (par exemple, <code>\$.requestParameters.bucketName</code>). Renvoie la valeur sous forme de chaîne.

Fonction	Renvoie	Description
<code>json_collect_values(json, path, field)</code>	Tableau	Accède à un tableau dans un document JSON et collecte le champ spécifié pour chaque élément. Cette fonction extrait une liste de valeurs à partir de structures répétées telles que les déclarations de politique IAM ou les règles des groupes de sécurité.
<code>get_aws_principal(policy_json, effect)</code>	Tableau	Analyse une politique de ressources IAM, Amazon S3 ou Lambda et renvoie les principaux du AWS compte à partir d'instructions correspondant à l'effet spécifié (Allow ou Deny). Cette fonction détecte l'accès entre comptes dans les politiques de ressources.
<code>policy_has_public_principal(policy_json, effect)</code>	Booléen	Renvoie true lorsqu'une instruction ayant l'effet spécifié accorde l'accès à un principal public ("*"). Cette fonction détecte les politiques qui autorisent l'accès public.
<code>RE2_FIND(input, pattern)</code>	Booléen	Renvoie vrai lorsque l'expression régulière RE2 pattern correspond à une partie de input. La correspondance fait la distinction majuscules/minuscules. Renvoie faux lorsque la valeur input est nulle. Les règles de surveillance du temps d'exécution utilisent cette fonction principalement pour faire correspondre les lignes de commande des processus.
<code>IRE2_FIND(input, pattern)</code>	Booléen	Identique RE2_FIND, mais la correspondance ne fait pas la distinction majuscules/minuscules.

L'agent GuardDuty de sécurité enregistre les arguments de ligne de commande d'un processus séparés par des caractères nuls. La plupart des règles de surveillance du temps d'exécution qui correspondent à une ligne de commande remplacent d'abord ces séparateurs par des espaces, par exemple `RE2_FIND(REPLACE(process.cmd_line, '\u0000', ' '), pattern)`.

La logique de détection SQL pour les règles de surveillance du temps d'exécution est une approximation de la manière dont l'activité est GuardDuty détectée, et non la logique exacte.

Gestion des règles de détection personnalisées

GuardDuty applique une règle à un compte par le biais d'une association. Une association lie une règle à votre compte et enregistre le mode (en direct ou à sec) dans lequel la règle fonctionne.

Dans une organisation, le compte d' GuardDuty administrateur délégué utilise les configurations de l'organisation pour gérer de manière centralisée les règles relatives aux comptes des membres. La configuration d'une organisation prend en charge les listes d'inclusion et d'exclusion pour contrôler les comptes auxquels s'applique une règle. Pour plus d'informations, consultez [Gestion des règles de détection personnalisées dans les environnements à comptes multiples](#).

Liste des règles disponibles

Le catalogue de règles répertorie toutes les règles disponibles, avec des filtres par nom, gravité, source de données, tactique MITRE ATT&CK®, technique et AWS service.

Console

Pour répertorier les règles disponibles

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Règles de détection personnalisées.
3. Utilisez les commandes de filtrage pour affiner la liste par propriété (par exemple, gravité ou tactique).

API/CLI

Lancez l'[ListCustomDetectionRules](#)opération. Vous pouvez appliquer des filtres pour affiner les résultats par nom, gravité, source de données, tactique, technique ou service.

```
aws guardduty list-custom-detection-rules \  
  --filters Name=severity,Values=HIGH
```

Affichage de l'état des règles

Chaque règle de votre compte possède l'un des trois statuts suivants :

- En direct : la règle est associée en mode direct et génère des résultats.
- Fonctionnement à sec : la règle est associée en mode de fonctionnement à sec et émet uniquement CloudWatch des métriques Amazon.
- Désactivé : la règle n'a aucune association et n'est pas évaluée.

Console

La colonne État de la page Règles de détection personnalisées indique le statut actuel de chaque règle. Vous pouvez filtrer par statut à l'aide de la liste déroulante.

API/CLI

Exécutez l'[ListCustomDetectionRuleAssociations](#) opération pour voir quelles règles sont associées à votre compte et à leur mode actuel.

```
aws guardduty list-custom-detection-rule-associations
```

Opérations en vrac

Les opérations groupées appliquent le même changement de mode à plusieurs règles ou à une règle appliquée à plusieurs comptes.

Console

Sur la page Règles de détection personnalisées, sélectionnez plusieurs règles à l'aide des cases à cocher, puis choisissez Actions pour activer ou désactiver toutes les règles sélectionnées en une seule action.

API/CLI

Pour appliquer la même modification à plusieurs règles, appelez [CreateCustomDetectionRuleAssociation](#) une fois par règle.

```
for RULE in rule-id-1 rule-id-2; do  
    aws guardduty create-custom-detection-rule-association \  
        --rule-id "$RULE" \  
done
```

```
--mode LIVE  
done
```

Pour couvrir toutes les règles du catalogue plutôt qu'une liste de noms, remplacez les ID des règles par le résultat de [ListCustomDetectionRules](#):`$(aws guardduty list-custom-detection-rules --query 'Rules[].RuleId' --output text)`.

Pour appliquer une règle unique à de nombreux comptes, utilisez une configuration organisationnelle plutôt que des appels par compte. Une configuration d'organisation cible les comptes membres avec des listes d'inclusion et d'exclusion, et GuardDuty crée les associations individuelles. Pour plus d'informations, consultez [Gestion des règles de détection personnalisées dans les environnements à comptes multiples](#).

Course à sec

En mode de fonctionnement à sec, GuardDuty évalue les événements par rapport à la règle mais ne génère pas de résultats. GuardDuty Émet plutôt des CloudWatch métriques Amazon que vous pouvez utiliser pour évaluer le volume du signal et le comportement des règles avant d'activer la détection en direct. GuardDuty publie ces statistiques uniquement lorsque la règle correspond à un événement ; si une règle ne correspond jamais, elle ne produit aucune métrique de course à sec.

Utilisez le mode d'exécution à sec pour comprendre le comportement d'une règle dans votre environnement sans déclencher de réponses automatisées ni générer de résultats dans la console.

Note

Une association de production à sec expire 14 jours après sa création. À son expiration, GuardDuty arrête d'évaluer la règle pour ce compte et la règle redevient désactivée. Pour réévaluer la règle, créez une nouvelle association de course à sec. Les associations actives n'expirent pas.

Console

Pour activer une règle en mode de fonctionnement à sec

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Règles de détection personnalisées.

3. Sélectionnez une ou plusieurs règles.
4. Choisissez Actions, puis sélectionnez Activer (Exécution à sec).

API/CLI

Exécutez l'[CreateCustomDetectionRuleAssociation](#) opération avec mode set to DRY_RUN.

```
aws guardduty create-custom-detection-rule-association \  
  --rule-id rule-id \  
  --mode DRY_RUN
```

Direct

En mode live, GuardDuty génère des résultats qui apparaissent dans la GuardDuty console. Les résultats sont exportés vers Amazon EventBridge et, si vous en configurez un, vers un compartiment Amazon S3 dont vous êtes le propriétaire. Les résultats sont également envoyés à AWS des services intégrés tels que AWS Security Hub. Utilisez le mode live pour détecter activement les menaces dans votre environnement.

Console

Pour activer une règle en mode actif

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Règles de détection personnalisées.
3. Sélectionnez une ou plusieurs règles.
4. Choisissez Actions, puis sélectionnez Activer (en direct).

Pour passer d'une règle existante d'une règle d'exploitation à sec à une règle dynamique, sélectionnez la règle, choisissez Actions, puis sélectionnez Activer (en direct).

API/CLI

Pour activer une nouvelle règle en mode actif, exécutez

l'[CreateCustomDetectionRuleAssociation](#) opération avec mode set to LIVE.

```
aws guardduty create-custom-detection-rule-association \  
  --rule-id rule-id \  
  --mode LIVE
```



```
--rule-id rule-id \  
--mode LIVE
```

Pour passer d'une règle existante d'une règle de fonctionnement à sec à une règle active, exécutez l'[UpdateCustomDetectionRuleAssociation](#) opération.

Désactivation des règles

La désactivation d'une règle supprime l'association et GuardDuty empêche l'évaluation des événements par rapport à cette règle pour votre compte.

Console

Pour désactiver les règles de détection personnalisées

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Règles de détection personnalisées.
3. Sélectionnez une ou plusieurs règles que vous souhaitez désactiver.
4. Choisissez Actions, puis sélectionnez Désactiver.
5. Confirmez l'action lorsque vous y êtes invité.

API/CLI

Lancez l'[DeleteCustomDetectionRuleAssociation](#) opération.

```
aws guardduty delete-custom-detection-rule-association \  
--rule-id rule-id
```

Gestion des règles de détection personnalisées dans les environnements à comptes multiples

Dans une organisation, le compte GuardDuty administrateur délégué gère les règles de détection personnalisées pour les comptes des membres de manière centralisée à l'aide des configurations de l'organisation. L'administrateur déclare l'intention de chaque règle et l' GuardDuty applique automatiquement aux comptes des membres, y compris aux comptes qui se joignent ultérieurement.

 Note

Multi-account la gestion des règles de détection personnalisées n'est prise en charge que pour les comptes gérés via AWS Organizations. Invitation-based les comptes membres ne sont pas pris en charge pour la gestion centralisée des règles.

Configurations d'organisation

Un compte membre ne peut pas activer, désactiver ou modifier lui-même une règle de détection personnalisée. Si vous tentez d'appeler les opérations d'association à compte unique depuis le compte d'un membre, GuardDuty renvoie un `AccessDeniedException` message d'erreur. L'administrateur gère la règle au nom du membre. Pour plus d'informations sur les comptes d'administrateur délégué et de membre, consultez [la section Gestion de plusieurs comptes dans GuardDuty](#).

Une configuration d'organisation lie une seule règle à un ensemble de comptes de membres. Il enregistre le mode, en direct ou à sec, dans lequel la règle s'applique à ces comptes. GuardDuty crée ensuite une association individuelle pour la règle dans chaque compte membre ciblé. Vous pouvez configurer des règles pour tous les membres ou pour des comptes spécifiques en utilisant des listes d'inclusion et d'exclusion.

Console

Pour configurer une règle de détection personnalisée pour l'organisation

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, sélectionnez Règles de détection personnalisées.
3. Choisissez un nom de règle pour ouvrir les détails de la règle, puis cliquez sur l'onglet Comptes.
4. Choisissez Configurer à côté de Configuration de l'organisation.
5. Sélectionnez le mode (Live ou Dry run) et choisissez les comptes à inclure ou à exclure.

API/CLI

Création d'une configuration d'organisation

Exécutez [CreateCustomDetectionRuleOrgConfiguration](#) pour créer une configuration de règles pour les comptes des membres.

Mettre à jour la configuration d'une organisation

Exécutez [UpdateCustomDetectionRuleOrgConfiguration](#) pour modifier le mode ou la portée du compte.

Supprimer la configuration d'une organisation

Exécutez [DeleteCustomDetectionRuleOrgConfiguration](#) pour supprimer la configuration de l'organisation. Comme une règle ne peut contenir qu'une configuration par mode, elle mode sélectionne celle à supprimer ; l'autre est laissée en place.

Note

La suppression d'une configuration d'organisation n'entraîne pas la suppression en cascade des associations de comptes membres existantes. La règle reste activée dans les comptes membres où elle est GuardDuty déjà appliquée.

Note

Une configuration d'organisation fonctionnant à sec expire 14 jours après sa création. Les associations de comptes membres GuardDuty créées à partir de cette configuration expirent avec elle, au lieu de 14 jours après la création de chaque association.

Exécution des deux modes pour la même règle

Une règle contient au maximum une configuration d'organisation par mode, de sorte qu'une règle peut s'exécuter en mode actif et en mode d'exécution à sec en même temps, uniquement à la condition suivante : les deux configurations doivent nommer leurs comptes cibles avec une liste d'inclusion explicite.

Une configuration qui affirme que l'ensemble de l'organisation est à la hauteur de ses règles. Une configuration prend en charge l'ensemble de l'organisation lorsqu'elle ne nomme aucun compte ou lorsqu'elle désigne des comptes à exclure. Aucune configuration pour l'autre mode ne peut coexister avec celui-ci, et la tentative d'en créer un revient à `ConflictException`. Pour déplacer une configuration de l'ensemble de l'organisation vers un autre mode, mettez à jour la configuration existante au lieu d'en créer une seconde.

Exemple : appliquer une règle en mode « run à sec » à tous les comptes membres

La commande AWS CLI suivante crée une configuration d'organisation qui cible tous les comptes membres, y compris les comptes qui se joignent ultérieurement. En omettant les deux `--include-account-ids` et en `--exclude-account-ids` ciblant l'ensemble de l'organisation.

```
aws guardduty create-custom-detection-rule-org-configuration \
  --rule-id "EXAMPLE_RULE_ID" \
  --mode DRY_RUN
```

Pour faire passer la règle à la détection en direct, mettez à jour la configuration existante avec [UpdateCustomDetectionRuleOrgConfiguration](#).

Appliquer toutes les règles au sein d'une organisation

La console configure une règle à la fois. Pour appliquer le même mode à toutes les règles disponibles au sein de l'organisation, parcourez le catalogue de règles à l'aide de la AWS CLI. En omettant les deux `--include-account-ids` et en `--exclude-account-ids` ciblant tous les comptes membres, y compris les comptes qui s'inscrivent ultérieurement.

```
for RULE in $(aws guardduty list-custom-detection-rules \
  --query 'Rules[].RuleId' --output text); do
  aws guardduty create-custom-detection-rule-org-configuration \
    --rule-id "$RULE" \
    --mode DRY_RUN
done
```

Cette boucle vous permet de mesurer le volume du signal avant qu'une règle ne génère de résultats. `--mode DRY_RUN` Comme la boucle ne nomme aucun compte, chaque configuration prend en charge l'ensemble de l'organisation et correspond à sa règle. Lorsque vous êtes prêt,

déplacez chaque règle vers la détection en direct en mettant à jour la configuration existante avec [UpdateCustomDetectionRuleOrgConfiguration](#). Réexécuter la boucle avec des `--mode LIVE` retourne `ConflictException`, car la configuration de fonctionnement à sec pour l'ensemble de l'organisation existe déjà.

Gérer plusieurs comptes sur Amazon GuardDuty

Lorsque votre AWS environnement comporte plusieurs comptes, vous pouvez les gérer en désignant un Compte AWS comme compte administrateur. Vous pouvez ensuite associer le multiple Comptes AWS à ce compte administrateur en tant que comptes de membre. Grâce à cette configuration, un compte GuardDuty administrateur désigné peut évaluer et surveiller la sécurité globale de votre organisation. Le compte administrateur peut également effectuer des tâches de gestion du compte, telles que l'examen de tous les résultats générés et la configuration des plans de protection qu'il contient GuardDuty.

Dans GuardDuty, une organisation se compose d'un compte d' GuardDuty administrateur délégué et d'un ou de plusieurs comptes de membres associés. Vous pouvez associer les comptes de deux manières : en les intégrant à AWS Organizations la console ou en utilisant une ancienne méthode d'envoi et d'acceptation des invitations d'adhésion dans la GuardDuty console. GuardDuty vous recommande de l'intégrer à AWS Organizations.

Note

Le bouton Modifier dans la section d'activation automatique de la page Comptes vous redirige vers la [Configuration des plans de protection](#) page au lieu d'ouvrir l'ancien modal de configuration.

AWS Organizations est un service mondial de gestion de comptes qui permet aux AWS administrateurs de consolider et de gérer de manière centralisée plusieurs comptes Comptes AWS. Il fournit des fonctionnalités de gestion des comptes et de facturation consolidée conçues pour répondre aux besoins budgétaires, de sécurité et de conformité. Il est proposé sans frais supplémentaires et s'intègre à plusieurs Services AWS applications, notamment Macie et Amazon GuardDuty. AWS Security Hub CSPM Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Organizations](#).

Table des matières

- [Comprendre la relation entre le compte GuardDuty administrateur et les comptes membres](#)
- [Gérer des GuardDuty comptes avec AWS Organizations](#)
- [Gestion des comptes à l'aide des politiques de l'organisation](#)
- [Gestion GuardDuty des comptes sur invitation](#)

- [GuardDuty considérations relatives à l'exportation des détails du compte d'un membre au format CSV](#)

Comprendre la relation entre le compte GuardDuty administrateur et les comptes membres

Lorsque vous l'utilisez GuardDuty dans un environnement à comptes multiples, le compte administrateur peut gérer certains aspects des comptes membres pour GuardDuty le compte des membres. Un compte administrateur peut exécuter les principales fonctions suivantes :

- Ajouter et supprimer des comptes de membres associés : le processus par lequel un compte administrateur peut effectuer cette opération varie en fonction de la façon dont vous gérez les comptes, que ce soit par le biais de la méthode d' GuardDuty invitation AWS Organizations ou par invitation.

GuardDuty recommande de gérer vos comptes de membres via AWS Organizations.

- Activation du compte d' GuardDuty administrateur délégué GuardDuty dans le compte de AWS Organizations gestion : si le compte de gestion est désactivé GuardDuty, le compte d' GuardDuty administrateur délégué peut être activé GuardDuty dans le compte de gestion. Cependant, il est nécessaire que le compte de gestion n'ait pas explicitement supprimé le [Service-linked autorisations de rôle pour GuardDuty](#).
- Configurer le statut des comptes membres — Un compte administrateur peut activer ou désactiver l'état des plans de GuardDuty protection, et activer, suspendre ou désactiver le statut de pour GuardDuty le compte des comptes membres associés.

Le compte GuardDuty d'administrateur délégué géré avec AWS Organizations peut être automatiquement activé GuardDuty lorsqu'ils Comptes AWS sont ajoutés en tant que membres.

- Personnaliser le moment de génération des résultats : un compte administrateur peut personnaliser les résultats au sein du GuardDuty réseau en créant et en gérant des règles de suppression, des listes d'adresses IP fiables et des listes de menaces. Dans un environnement à comptes multiples, la prise en charge de la configuration de ces fonctionnalités n'est disponible que pour un compte d' GuardDuty administrateur délégué. Un compte membre ne peut pas mettre à jour cette configuration.

Le tableau suivant décrit la relation entre le compte GuardDuty administrateur et les comptes membres.

Clé pour la table

- Auto-utilisateur : un compte ne peut effectuer l'action répertoriée que pour son propre compte.
- N'importe lequel : un compte peut exécuter l'action répertoriée pour n'importe quel compte associé.
- Tout — Un compte peut effectuer l'action répertoriée et elle s'applique à tous les comptes associés. Généralement, le compte effectuant cette action est un compte GuardDuty administrateur désigné
- Cellules avec tiret (—) — Les cellules du tableau avec tiret (—) indiquent que le compte ne peut pas effectuer l'action répertoriée.

Action	À travers AWS Organizations		Sur invitation	
	Compte GuardDuty d'administrateur délégué	Compte de membre associé	GuardDuty compte administrateur	Compte de membre associé
Activer GuardDuty	N'importe lequel	—	Auto-utilisateur	Self
GuardDuty Activation automatique pour l'ensemble de l'organisation (ALL,NEW,NONE)	Tous	—	—	—
Afficher les comptes de tous les membres des Organisations, quel que soit leur GuardDuty statut	N'importe lequel	—	—	—
Générer des échantillons de résultats	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Self

Afficher tous les GuardDuty résultats	N'importe lequel	Self	N'importe lequel	Self
GuardDuty Conclusions des archives	N'importe lequel	–	N'importe lequel	–
Appliquer des règles de suppression	Tous	–	Tous	–
Créez une liste d'adresses IP fiables ou des listes de menaces	Tous	–	Tous	–
Mettre à jour la liste d'adresses IP fiables ou les listes de menaces	Tous	–	Tous	–
Supprimer la liste d'adresses IP fiables ou les listes de menaces	Tous	–	Tous	–
Définissez la fréquence des EventBridge notifications	Tous	–	Tous	–

Définir l'emplacement Amazon S3 pour l'exportation des résultats	Tous	Auto-utilisateur	Auto-utilisateur	Self
Activez un ou plusieurs plans de protection facultatifs pour l'ensemble de l'entreprise (ALL,NEW,NONE)	Tous	–	–	–
Cela n'inclut pas la protection contre les programmes malveillants pour S3.				
Activez n'importe quel plan de GuardDuty protection pour les comptes individuels	N'importe lequel	–	N'importe lequel	–
Cela n'inclut pas la protection contre les programmes malveillants pour EC2 et la protection contre les logiciels malveillants pour S3.				

Protection contre les logiciels malveillants pour EC2	N'importe lequel	–	Self	–
Protection contre les programmes malveillants pour EC2 : analyse des On-demand programmes malveillants	N'importe lequel	Auto-utilisateur	Auto-utilisateur	Self
Protection contre les logiciels malveillants pour S3	–	Auto-utilisateur	–	Self
Dissocier un compte membre	N'importe lequel ⁺	–	N'importe lequel	–
Dissocier d'un compte administrateur	–	–	–	Self
Supprimer un compte de membre dissocié	N'importe lequel	–	N'importe lequel	–
Suspendre GuardDuty	N'importe lequel [*]	–	N'importe lequel [*]	–
Désactiver GuardDuty	N'importe lequel [*]	–	N'importe lequel [*]	Self

⁺ Indique que le compte GuardDuty administrateur délégué ne peut effectuer cette action que s'il n'a pas configuré les préférences d'activation automatique pour ALL les membres de l'organisation.

* Indique qu'un compte d' GuardDuty administrateur délégué ne peut pas être désactivé directement GuardDuty dans un compte de membre. Le compte GuardDuty d'administrateur délégué doit d'abord dissocier le compte du membre, puis le supprimer. Ensuite, chaque compte membre peut être désactivé GuardDuty dans son propre compte. Pour plus d'informations sur l'exécution de ces tâches dans votre organisation, consultez [Gérez en permanence vos comptes de membres au sein de GuardDuty](#).

Comprendre l'état de la relation avec les membres

GuardDuty Les opérations d'API telles que [ListMembers](#) et [GetMembers](#) renvoient un `relationshipStatus` champ pour chaque compte membre. Ce champ indique l'état actuel de la relation entre le compte administrateur et le compte membre. Vérifiez cette valeur lorsque vous souhaitez confirmer que le compte d'un membre GuardDuty est activement surveillé. Cela vous aide également à résoudre les problèmes liés au fait qu'un compte membre n'a pas terminé son intégration ou n'est plus surveillé. La liste suivante décrit les valeurs possibles.

Created

Le compte administrateur a ajouté ce compte en tant que membre (par exemple, en appelant `CreateMembers`), mais la relation de membre n'est pas encore active.

Invited

Le compte administrateur a envoyé une invitation à ce compte membre, et l'invitation attend d'être acceptée.

Enabled

Ce compte de membre est associé au compte d'administrateur et GuardDuty surveille activement le compte de membre.

Disabled

Ce compte de membre est associé au compte d'administrateur, mais GuardDuty ne surveille pas activement le compte de membre.

Removed

Ce compte de membre n'est plus associé au compte d'administrateur. Ce statut indique généralement que le compte administrateur a supprimé l'association.

Resigned

Ce compte de membre n'est plus associé au compte d'administrateur. Ce statut indique généralement que le compte du membre s'est retiré de l'association.

Deleted

Ce compte de membre n'existe plus dans GuardDuty.

EmailVerificationInProgress

L'invitation de ce compte membre est en attente de vérification de l'adresse e-mail.

EmailVerificationFailed

L'invitation de ce compte membre n'a pas été validée par e-mail.

RegionDisabled

Ce compte de membre ne peut pas être surveillé car il GuardDuty n'est pas activé ou n'est pas disponible actuellement Région AWS.

AccountSuspended

Celui de ce membre Compte AWS est suspendu.

CannotCreateDetectorInOrganizationMasterAccount

GuardDuty ne peut pas créer de détecteur dans le compte AWS Organizations de gestion, généralement parce que les autorisations requises pour les rôles liés au service sont manquantes.

Gérer des GuardDuty comptes avec AWS Organizations

Dans une AWS organisation, le compte de gestion peut désigner n'importe quel compte au sein de cette organisation comme compte d' GuardDuty administrateur délégué. Pour ce compte administrateur, GuardDuty il est activé automatiquement uniquement dans le cas actuel Région AWS. Par défaut, le compte administrateur peut activer et gérer tous GuardDuty les comptes membres de l'organisation au sein de cette région. Le compte administrateur peut consulter et ajouter des membres à cette AWS organisation.

Les sections suivantes vous guideront à travers les différentes tâches que vous pouvez effectuer en tant que compte d' GuardDuty administrateur délégué.

Table des matières

- [Considérations et recommandations d'utilisation GuardDuty avec AWS Organizations](#)
- [Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué](#)
- [Désignation d'un compte d'administrateur délégué GuardDuty](#)
- [Configuration des préférences d'activation automatique de l'organisation](#)
- [Ajouter des membres à l'organisation](#)
- [\(Facultatif\) Activez les plans de protection pour les comptes de membres existants](#)
- [Gérez en permanence vos comptes de membres au sein de GuardDuty](#)
- [Suspension GuardDuty pour compte membre](#)
- [Dissociation \(suppression\) du compte membre du compte administrateur](#)
- [Supprimer des comptes de membres de GuardDuty l'organisation](#)
- [Modification du compte GuardDuty d'administrateur délégué](#)

Considérations et recommandations d'utilisation GuardDuty avec AWS Organizations

Les considérations et recommandations suivantes peuvent vous aider à comprendre le fonctionnement d'un compte d' GuardDuty administrateur délégué dans GuardDuty :

Un compte d' GuardDuty administrateur délégué peut gérer un maximum de 50 000 membres.

Il y a une limite de 50 000 comptes membres par compte GuardDuty d'administrateur délégué. Cela inclut les comptes de membres ajoutés par le biais du compte GuardDuty administrateur AWS Organizations ou ceux qui ont accepté l'invitation du compte administrateur à rejoindre leur organisation. Toutefois, votre AWS organisation peut compter plus de 50 000 comptes.

Si vous dépassez la limite de 50 000 comptes membres, vous recevrez une notification et un e-mail du compte d' GuardDuty administrateur délégué désigné. CloudWatch Tableau de bord Health

Un compte GuardDuty d'administrateur délégué est régional.

Contrairement AWS Organizations à GuardDuty un service régional. Les comptes d' GuardDuty administrateur délégué et leurs comptes de membre doivent être ajoutés AWS Organizations dans chaque région souhaitée dans laquelle vous avez GuardDuty activé votre compte. Si le compte de gestion de l'organisation désigne un compte d' GuardDuty administrateur délégué uniquement dans l'est des États-Unis (Virginie du Nord), le compte d' GuardDuty administrateur

délégué gèrera uniquement les comptes des membres ajoutés à l'organisation dans cette région. Pour plus d'informations sur la parité des fonctionnalités dans les régions où GuardDuty elle est disponible, consultez [Régions et points de terminaison](#).

Cas particuliers pour les régions optionnelles

- Lorsqu'un compte d' GuardDuty administrateur délégué se retire d'une région optionnelle, même si la configuration d' GuardDuty activation automatique de votre organisation est définie sur les nouveaux comptes membres uniquement (NEW) ou sur tous les comptes membres (ALL), il GuardDuty ne peut être activé pour aucun compte de membre de l'organisation actuellement désactivé. GuardDuty Pour plus d'informations sur la configuration de vos comptes membres, ouvrez Comptes dans le volet de navigation de la [GuardDuty console](#) ou utilisez l'[ListMembersAPI](#).
- Lorsque vous travaillez avec la configuration GuardDuty d'activation automatique définie sur NEW, assurez-vous que la séquence suivante est respectée :
 1. Les comptes membres optent pour une région optionnelle.
 2. Ajoutez les comptes des membres à votre organisation dans AWS Organizations.

Si vous modifiez l'ordre de ces étapes, le paramètre d' GuardDuty activation automatique ne **NEW** fonctionnera pas dans la région d'inscription spécifique, car le compte du membre n'est plus nouveau pour l'organisation. GuardDuty propose deux solutions alternatives :

- Définissez la configuration GuardDuty d'activation automatique sur ALL, qui inclut les comptes de membres nouveaux et existants. Dans ce cas, l'ordre de ces étapes n'est pas pertinent.
- Si un compte membre fait déjà partie de votre organisation, gérez la GuardDuty configuration de ce compte individuellement dans la région d'adhésion spécifique à l'aide de la GuardDuty console ou de l'API.

Nécessaire pour qu'une AWS organisation dispose du même compte GuardDuty d'administrateur délégué pour tous les Régions AWS.

Vous devez désigner un compte membre comme compte d' GuardDuty administrateur délégué pour tous les comptes Régions AWS GuardDuty Where activé. Par exemple, si vous désignez un compte de membre **111122223333** dans **Europe (Ireland)**, vous ne pouvez pas désigner un autre compte de membre **555555555555** dans **Canada (Central)**. Vous devez utiliser le même compte que le compte d' GuardDuty administrateur délégué dans toutes les autres régions.

Vous pouvez désigner un nouveau compte GuardDuty d'administrateur délégué à tout moment. Pour plus d'informations sur la suppression du compte GuardDuty administrateur délégué existant, consultez [Modification du compte GuardDuty d'administrateur délégué](#).

Il n'est pas recommandé de définir le compte de gestion de votre organisation comme compte GuardDuty d'administrateur délégué.

Le compte de gestion de votre organisation peut être le compte GuardDuty d'administrateur délégué. Cependant, les bonnes pratiques de sécurité AWS suivent le principe du moindre privilège et ne recommandent pas cette configuration.

La modification d'un compte d' GuardDuty administrateur délégué n'est pas désactivée GuardDuty pour les comptes des membres.

Si vous supprimez un compte d' GuardDuty administrateur délégué, GuardDuty tous les comptes de membre associés à ce compte d' GuardDuty administrateur délégué sont supprimés. GuardDuty reste activé pour tous ces comptes de membres.

Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué

Pour commencer à utiliser Amazon GuardDuty avec AWS Organizations, le compte AWS Organizations de gestion de l'organisation désigne un compte en tant que compte d' GuardDuty administrateur délégué. Cela permet GuardDuty en tant que service fiable de AWS Organizations. Il active également le compte GuardDuty d' GuardDuty administrateur délégué et permet également au compte d'administrateur délégué d'activer et de gérer GuardDuty d'autres comptes de l'organisation dans la région actuelle. Pour plus d'informations sur la manière dont ces autorisations sont accordées, consultez la section [Utilisation AWS Organizations avec d'autres AWS services](#).

En tant que compte de AWS Organizations gestion, avant de désigner le compte d' GuardDuty administrateur délégué pour votre organisation, vérifiez que vous pouvez effectuer l' GuardDuty action suivante : `guardduty:EnableOrganizationAdminAccount` Cette action vous permet de désigner le compte d' GuardDuty administrateur délégué pour votre organisation en utilisant GuardDuty. Vous devez également vous assurer que vous êtes autorisé à effectuer les AWS Organizations actions qui vous aident à récupérer des informations sur votre organisation.

Pour accorder ces autorisations, incluez la déclaration suivante dans une politique Gestion des identités et des accès AWS (IAM) pour votre compte :

```
{
  "Sid": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
```



```

    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:ListRoots"
  ],
  "Resource": "*"
}

```

Si vous souhaitez désigner votre compte AWS Organizations de gestion comme compte d' GuardDuty administrateur délégué, votre compte aura également besoin de l'action IAM :CreateServiceLinkedRole. Cette action vous permet d'initialiser le compte GuardDuty de gestion. Cependant, vérifiez [Considérations et recommandations d'utilisation GuardDuty avec AWS Organizations](#) avant de procéder à l'ajout des autorisations.

Pour continuer à désigner le compte de gestion comme compte d' GuardDuty administrateur délégué, ajoutez la déclaration suivante à la politique IAM et **111122223333** remplacez-la par l' Compte AWS ID du compte de gestion de votre organisation :

```

{
  "Sid": "PermissionsToEnableGuardDuty"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "guardduty.amazonaws.com"
    }
  }
}

```

Désignation d'un compte d'administrateur délégué GuardDuty

Cette section décrit les étapes à suivre pour désigner un administrateur délégué au GuardDuty sein de l'organisation.

En tant que compte de gestion de l' AWS organisation, assurez-vous de lire attentivement [Considérations et recommandations](#) le mode de fonctionnement d'un compte d' GuardDuty administrateur délégué. Avant de continuer, assurez-vous que vous avez [Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué](#).

Choisissez une méthode d'accès préférée pour désigner un compte d' GuardDuty administrateur délégué pour votre organisation. Seul un compte de gestion peut effectuer cette étape.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte de gestion de votre AWS Organizations organisation.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désigner le compte d' GuardDuty administrateur délégué pour votre organisation.
3. Procédez de l'une des manières suivantes, selon que votre compte de gestion GuardDuty est activé ou non dans la région actuelle :
 - Si GuardDuty ce n'est pas activé, sélectionnez Amazon GuardDuty - toutes les fonctionnalités, puis choisissez Get started. Cette action vous redirigera vers la GuardDuty page de bienvenue.
 - Si cette option GuardDuty est activée, choisissez Paramètres dans le volet de navigation.
4. Sous Administrateur délégué, entrez l' Compte AWS ID à 12 chiffres du compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué pour l'organisation.
5. Choisissez Delegate (Déléguer).
6. (Recommandé) Répétez les étapes précédentes pour désigner le compte d' GuardDuty administrateur délégué dans chaque Région AWS endroit où vous avez GuardDuty activé le compte.

API/CLI

1. [enableOrganizationAdminAccount](#) Exécuté en utilisant les informations d'identification Compte AWS du compte de gestion de l'organisation.
 - Vous pouvez également utiliser AWS Command Line Interface pour cela. La AWS CLI commande suivante désigne un compte d' GuardDuty administrateur délégué pour votre région actuelle uniquement. Exécutez la AWS CLI commande suivante et assurez-vous de le **111111111111** remplacer par l' Compte AWS ID du compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué :

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

Pour désigner le compte d' GuardDuty administrateur délégué pour les autres régions, spécifiez la région dans la AWS CLI commande. L'exemple suivant montre comment activer un compte d' GuardDuty administrateur délégué dans l'ouest des États-Unis (Oregon). Assurez-vous de le **us-west-2** remplacer par la région à laquelle vous souhaitez attribuer le compte d' GuardDuty administrateur délégué.

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

Pour plus d'informations sur l' Régions AWS endroit où GuardDuty est disponible, consultez [Régions et points de terminaison](#).

S' GuardDuty il est désactivé pour votre compte d' GuardDuty administrateur délégué, il ne pourra effectuer aucune action. Si ce n'est pas déjà fait, assurez-vous GuardDuty d'activer le compte d' GuardDuty administrateur délégué nouvellement désigné.

2. (Recommandé) Répétez les étapes précédentes pour désigner le compte d' GuardDuty administrateur délégué dans chaque Région AWS cas où vous l'avez GuardDuty activé.

Configuration des préférences d'activation automatique de l'organisation

La fonctionnalité d'activation automatique de l'organisation vous GuardDuty permet de définir le même statut GuardDuty et le statut des plans de protection pour ALL les comptes existants ou NEW membres de votre organisation, en une seule étape. De même, vous pouvez également spécifier à quel moment vous ne souhaitez effectuer aucune action sur les comptes des membres, en

choisissant NONE. Les étapes suivantes expliquent ces paramètres et indiquent également à quel moment vous souhaitez utiliser un paramètre spécifique.

Note

Vous pouvez définir les préférences d'activation automatique pour tous les plans de protection, à l'exception [Protection contre les logiciels malveillants pour S3](#) de.

Choisissez une méthode d'accès préférée pour mettre à jour les préférences d'activation automatique pour l'organisation.

Console

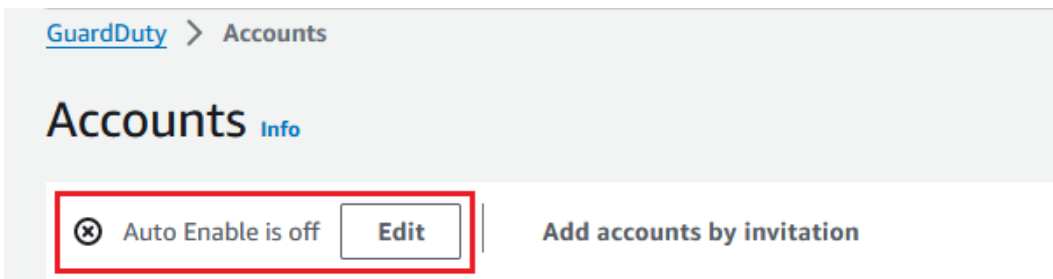
1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte GuardDuty administrateur.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

La page Comptes fournit des options de configuration pour le compte GuardDuty administrateur Auto-enable GuardDuty et les plans de protection facultatifs pour le compte des comptes membres appartenant à l'organisation.

3. Pour mettre à jour les paramètres d'activation automatique existants, choisissez Modifier.



Ce support est disponible pour configurer GuardDuty et tous les plans de protection optionnels pris en charge dans votre Région AWS. Vous pouvez sélectionner l'une des options de configuration suivantes pour GuardDuty le compte de vos comptes membres :

- Activer pour tous les comptes (**ALL**) : sélectionnez cette option pour activer l'option correspondante pour tous les comptes d'une organisation. Cela inclut les nouveaux comptes qui rejoignent l'organisation et ceux qui peuvent avoir été suspendus ou

supprimés de l'organisation. Cela inclut également le compte GuardDuty d'administrateur délégué.

 Note

La mise à jour de la configuration de tous les comptes membres peut prendre jusqu'à 24 heures.

- Auto-enable pour les nouveaux comptes (**NEW**) : sélectionnez cette option pour activer automatiquement les plans de protection GuardDuty ou les plans de protection facultatifs pour les nouveaux comptes uniquement lorsqu'ils rejoignent votre organisation.
- Ne pas activer (**NONE**) : sélectionnez cette option pour empêcher l'activation de l'option correspondante pour les nouveaux comptes de votre organisation. Dans ce cas, le compte GuardDuty administrateur gérera chaque compte individuellement.

Lorsque vous mettez à jour le paramètre d'activation automatique depuis ALL ou NEW vers NONE, cette action ne désactive pas l'option correspondante pour vos comptes existants. Cette configuration s'appliquera aux nouveaux comptes qui rejoignent l'organisation. Après avoir mis à jour les paramètres d'activation automatique, l'option correspondante ne sera activée pour aucun nouveau compte.

 Note

Lorsqu'un compte d'administrateur délégué se retire d'une région optionnelle, même si la configuration d'activation automatique de votre organisation est définie sur les nouveaux comptes membres uniquement (NEW) ou sur tous les comptes membres (ALL), il GuardDuty ne peut être activé pour aucun compte de membre de l'organisation actuellement désactivé. Pour plus d'informations sur la configuration de vos comptes membres, ouvrez Comptes dans le volet de navigation de la [GuardDuty console](#) ou utilisez l'[ListMembers API](#).

4. Cliquez sur Enregistrer les modifications.
5. (Facultatif) Si vous souhaitez utiliser les mêmes préférences dans chaque région, mettez à jour vos préférences séparément dans chacune des régions prises en charge.

Certains des plans de protection optionnels peuvent ne pas être disponibles partout Régions AWS où ils GuardDuty sont disponibles. Pour plus d'informations, consultez [Régions et points de terminaison](#).

API/CLI

1. Exécutez-le en [UpdateOrganizationConfiguration](#) utilisant les informations d'identification du compte d' GuardDuty administrateur délégué, afin de configurer GuardDuty automatiquement des plans de protection facultatifs dans cette région pour votre organisation. Pour plus d'informations sur les différentes configurations d'activation automatique, voir [automatique EnableOrganizationMembers](#).

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

Pour définir les préférences d'activation automatique pour l'un des plans de protection facultatifs pris en charge dans votre région, suivez les étapes indiquées dans les sections de documentation correspondantes de chaque plan de protection.

2. Vous pouvez valider les préférences de votre organisation dans la région actuelle. Exécutez [describeOrganizationConfiguration](#). Assurez-vous de spécifier l'ID du détecteur du compte d' GuardDuty administrateur délégué.

Note

La mise à jour de la configuration de tous les comptes membres peut prendre jusqu'à 24 heures.

3. Vous pouvez également exécuter la AWS CLI commande suivante pour définir les préférences afin d'activer ou de désactiver automatiquement GuardDuty dans cette région les nouveaux comptes (NEW) qui rejoignent l'organisation, tous les comptes (ALL) ou aucun des comptes (NONE) de l'organisation. Pour plus d'informations, voir [auto EnableOrganizationMembers](#). Selon vos préférences, vous devrez peut-être remplacer NEW par ALL ou NONE. Si vous configurez le plan de protection avecALL, le plan de protection sera également activé pour le compte d' GuardDuty administrateur délégué. Assurez-vous de spécifier l'ID du détecteur du compte d' GuardDuty administrateur délégué qui gère la configuration de l'organisation.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

4. Vous pouvez valider les préférences de votre organisation dans la région actuelle. Exécutez la AWS CLI commande suivante en utilisant l'ID du détecteur du compte GuardDuty administrateur délégué.

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```

(Recommandé) Répétez les étapes précédentes dans chaque région en utilisant l'identifiant du détecteur de compte GuardDuty administrateur délégué.

Note

Lorsqu'un compte d' GuardDuty administrateur délégué se retire d'une région optionnelle, même si la configuration d' GuardDuty activation automatique de votre organisation est définie sur les nouveaux comptes membres uniquement (NEW) ou sur tous les comptes membres (ALL), il GuardDuty ne peut être activé pour aucun compte de membre de l'organisation actuellement désactivé. GuardDuty Pour plus d'informations sur la configuration de vos comptes membres, ouvrez Comptes dans le volet de navigation de la [GuardDuty console](#) ou utilisez l'[ListMembers](#)API.

Ajouter des membres à l'organisation

En tant que compte d' GuardDuty administrateur délégué, vous pouvez en ajouter un ou plusieurs Comptes AWS à l' GuardDuty organisation. Lorsque vous ajoutez un compte en tant que GuardDuty membre, il sera automatiquement GuardDuty activé dans cette région. Il existe une exception au compte de gestion de l'organisation. Avant que le compte de gestion ne soit ajouté en tant que GuardDuty membre, il doit être GuardDuty activé.

Choisissez une méthode préférée pour ajouter un compte membre à votre GuardDuty organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guarddduty/>.

Pour vous connecter, utilisez les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

Le tableau des comptes affiche tous les comptes de membres actifs (non suspendus Comptes AWS) qui peuvent être associés au compte d' GuardDuty administrateur délégué. Si le compte membre est associé au compte administrateur de l'organisation, le type sera l'un des suivants : Via Organizations ou Par invitation. Si un compte membre n'est pas associé au compte GuardDuty administrateur de l'organisation, le type de ce compte de membre est Non membre.

3. Sélectionnez un ou plusieurs identifiants de compte que vous souhaitez ajouter en tant que membres. Ces ID de compte doivent avoir le Type Via les organisations.

Les comptes ajoutés par invitation ne font pas partie de votre organisation. Vous pouvez gérer ces comptes individuellement. Pour plus d'informations, consultez [Gestion des comptes par invitation](#).

4. Choisissez le menu déroulant Actions, puis sélectionnez Ajouter un membre. Après avoir ajouté ce compte en tant que membre, la GuardDuty configuration d'activation automatique s'applique. En fonction des paramètres définis dans [Configuration des préférences d'activation automatique de l'organisation](#), la GuardDuty configuration de ces comptes peut changer.
5. Vous pouvez sélectionner la flèche vers le bas de la colonne État pour trier les comptes en fonction du statut Non membre, puis choisir chaque compte qui n'est pas GuardDuty activé dans la région actuelle.

Si aucun des comptes répertoriés dans le tableau des comptes n'a encore été ajouté en tant que membre, vous pouvez activer tous les comptes de l'organisation GuardDuty dans la région actuelle. Dans la bannière en haut de la page, choisissez Activer. Cette action active automatiquement la Auto-enable GuardDuty configuration afin qu' GuardDuty elle soit activée pour tout nouveau compte qui rejoint l'organisation.

6. Choisissez Confirmer pour ajouter les comptes en tant que membres. Cette action active GuardDuty également tous les comptes sélectionnés. La valeur Statut des comptes invités devient Activé.

7. (Recommandé) Répétez ces étapes pour chacune d'entre elles Région AWS. Cela garantit que le compte d' GuardDuty administrateur délégué peut gérer les résultats et les autres configurations des comptes membres dans toutes les régions dans lesquelles vous l'avez GuardDuty activé.

La fonction d'activation automatique est accessible GuardDuty à tous les futurs membres de votre organisation. Cela permet à votre compte d' GuardDuty administrateur délégué de gérer tous les nouveaux membres créés au sein de l'organisation ou ajoutés à celle-ci. Lorsque le nombre de comptes de membres atteint la limite de 50 000, la Auto-enable fonctionnalité est automatiquement désactivée. Si vous supprimez un compte de membre et que le nombre total de membres tombe à moins de 50 000, la Auto-enable fonctionnalité est réactivée.

API/CLI

- [CreateMembers](#) Exécuté en utilisant les informations d'identification du compte GuardDuty d'administrateur délégué.

Vous devez spécifier l'ID de détecteur régional du compte d' GuardDuty administrateur délégué et les détails du compte (Compte AWS identifiants et adresses e-mail correspondantes) des comptes que vous souhaitez ajouter en tant que GuardDuty membres. Vous pouvez créer un ou plusieurs membres avec cette opération d'API.

Lorsque vous gérez CreateMembers au sein de votre organisation, les préférences d'activation automatique pour les nouveaux membres s'appliquent à mesure que de nouveaux comptes membres rejoignent votre organisation. Lorsque vous utilisez CreateMembers un compte de membre existant, la configuration de l'organisation s'applique également aux membres existants. Cela peut modifier la configuration actuelle des comptes membres existants.

Exécutez-le [ListAccounts](#) dans la référence d'AWS Organizations API pour afficher tous les comptes de l' AWS organisation.

- Vous pouvez également utiliser AWS Command Line Interface. Exécutez la commande AWS CLI suivante et assurez-vous d'utiliser votre propre ID de détecteur valide, votre ID Compte AWS et l'adresse e-mail associée à l'ID de compte.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

Vous pouvez consulter la liste de tous les membres de l'organisation en exécutant la AWS CLI commande suivante :

```
aws organizations list-accounts
```

Après avoir ajouté ce compte en tant que membre, la GuardDuty configuration d'activation automatique s'applique.

(Facultatif) Activez les plans de protection pour les comptes de membres existants

La procédure suivante inclut les étapes permettant d'activer les plans de protection pour les comptes de membres existants à l'aide de la page Comptes. Pour connaître les étapes à suivre à l'aide de l'API ou AWS CLI consultez les documents relatifs au plan de protection spécifique.

Vous pouvez activer les plans de protection pour des comptes individuels via la page Comptes.

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Utilisez les informations d'identification GuardDuty du compte administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sélectionnez un ou plusieurs comptes pour lesquels vous souhaitez configurer un plan de protection. Répétez les étapes suivantes pour chaque plan de protection que vous souhaitez configurer :
 - a. Choisissez Modifier les plans de protection.
 - b. Dans la liste des plans de protection, choisissez celui que vous souhaitez configurer.
 - c. Choisissez l'une des actions que vous souhaitez effectuer pour ce plan de protection, puis cliquez sur Confirmer.
 - d. Pour le compte sélectionné, la colonne correspondant au plan de protection configuré affichera la configuration mise à jour en tant que Activée ou Non activée.

Gérez en permanence vos comptes de membres au sein de GuardDuty

En tant que compte d' GuardDuty administrateur délégué, vous êtes chargé de gérer la configuration GuardDuty et les plans de protection facultatifs de tous les comptes pris en charge au sein de votre organisation Région AWS. Les sections suivantes présentent les options relatives au maintien de l'état de configuration de GuardDuty ou de l'un de ses plans de protection facultatifs :

Pour maintenir l'état de configuration de l'ensemble de votre organisation dans chaque région

- Définissez les préférences d'activation automatique pour l'ensemble de l'organisation à l'aide de la GuardDuty console : vous pouvez les activer GuardDuty automatiquement pour tous (ALL) les membres de l'organisation ou pour les nouveaux (NEW) membres qui rejoignent l'organisation, ou choisir de ne pas (NONE) l'activer automatiquement pour aucun des membres de l'organisation.

Vous pouvez également configurer des paramètres identiques ou différents pour tous les plans de protection inclus GuardDuty.

La mise à jour de la configuration de tous les comptes membres de l'organisation peut prendre jusqu'à 24 heures.

- Mettez à jour les préférences d'activation automatique à l'aide de l'API — Exécutez [UpdateOrganizationConfiguration](#) pour configurer automatiquement GuardDuty et ses plans de protection facultatifs pour l'organisation. Lorsque vous lancez [CreateMembers](#) pour ajouter de nouveaux comptes membres dans votre organisation, les paramètres configurés s'appliquent automatiquement. Lorsque vous utilisez CreateMembers un compte de membre existant, la configuration de l'organisation s'applique également aux membres existants. Cela peut modifier la configuration actuelle des comptes membres existants.

Pour afficher tous les comptes de votre organisation, lancez-vous [ListAccounts](#) dans la référence AWS Organizations d'API.

Pour maintenir l'état de configuration des comptes membres individuellement dans chaque région

- Pour afficher tous les comptes de votre organisation, lancez-vous [ListAccounts](#) dans la référence AWS Organizations d'API.
- Si vous souhaitez que les comptes de membres sélectionnés aient un statut de configuration différent, [UpdateMemberDetectors](#) exécutez-les individuellement pour chaque compte membre.

Vous pouvez utiliser GuardDuty la console pour effectuer la même tâche en accédant à la page Comptes de la GuardDuty console.

Pour plus d'informations sur l'activation des plans de protection pour des comptes individuels à l'aide de la console ou de l'API, consultez la page de configuration du plan de protection correspondant.

Suspension GuardDuty pour compte membre

En tant que compte d' GuardDuty administrateur délégué, vous pouvez suspendre le GuardDuty service pour un compte de membre de votre organisation. Dans ce cas, le compte du membre reste dans votre GuardDuty organisation. Vous pouvez également réactiver GuardDuty ces comptes de membres ultérieurement. Toutefois, si vous souhaitez finalement dissocier (supprimer) ce compte de membre, après avoir suivi les étapes de cette section, vous devez suivre les étapes décrites dans [Dissociation \(suppression\) du compte membre du compte administrateur](#).

Lorsque vous suspendez GuardDuty un compte membre, vous pouvez vous attendre aux modifications suivantes :

- GuardDuty ne surveille plus la sécurité de l' AWS environnement ou ne génère plus de nouvelles découvertes.
- Les résultats existants dans le compte du membre restent intacts.
- Un compte de membre GuardDuty suspendu n'entraîne aucun frais pour. GuardDuty

Si le compte membre a activé la protection contre les programmes malveillants pour S3 pour un ou plusieurs compartiments de son compte, la suspension GuardDuty n'a aucune incidence sur la configuration de Malware Protection pour S3. Le compte membre continuera à supporter les frais d'utilisation de Malware Protection for S3. Pour que le compte membre cesse d'utiliser Malware Protection for S3, il doit désactiver cette fonctionnalité pour les compartiments protégés. Pour plus d'informations, consultez [Désactivation de la protection contre les programmes malveillants pour S3 pour un compartiment protégé](#).

Choisissez la méthode préférée de suspension GuardDuty pour un compte membre de votre organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte d' GuardDuty administrateur délégué.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sur la page Comptes, sélectionnez un ou plusieurs comptes que vous souhaitez suspendre GuardDuty.
4. Choisissez le menu déroulant Actions, puis sélectionnez Suspendre GuardDuty.
5. Choisissez Suspendre GuardDuty pour confirmer la sélection.

Cela fera passer le statut du compte membre à Désactivé (suspendu).

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez dissocier ou supprimer le compte membre.

API

1. Pour récupérer l'identifiant du compte membre dont vous souhaitez suspendre le compte GuardDuty, utilisez l'[ListMembers](#) API. Incluez le `OnlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur `true`, GuardDuty renvoie un `members` tableau fournissant des détails uniquement sur les comptes actuellement GuardDuty membres.

Vous pouvez également utiliser AWS Command Line Interface (AWS CLI) pour exécuter la commande suivante :

```
aws guardduty list-members --only-associated true --region us-east-1
```

Remplacez *us-east-1* par la région où vous souhaitez suspendre GuardDuty ce compte.

2. Pour suspendre un ou plusieurs comptes de GuardDuty membre, lancez [StopMonitoringMembers](#) la procédure de suspension GuardDuty pour un compte de membre.

Vous pouvez également AWS CLI exécuter la commande suivante :

```
aws guardduty stop-monitoring-members --detector-id  
12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Remplacez *us-east-1* par la région dans laquelle vous souhaitez suspendre ce compte. Si vous avez une liste d'identifiants de compte que vous souhaitez supprimer, séparez-les par un espace.

Si vous souhaitez également dissocier (supprimer) ce compte membre, suivez les étapes décrites dans [Dissociation \(suppression\) du compte membre du compte administrateur](#).

Dissociation (suppression) du compte membre du compte administrateur

Lorsque vous souhaitez arrêter de configurer les GuardDuty paramètres et d'accéder aux données depuis un compte membre, supprimez ce compte en tant que compte GuardDuty membre. Vous pouvez le faire en dissociant (en supprimant) ce compte du compte GuardDuty administrateur.

Lorsque vous dissociez un compte GuardDuty membre, voici ce qui se passe :

- GuardDuty reste activé pour le compte en cours Région AWS, mais le compte est dissocié du compte d' GuardDuty administrateur délégué.
- Le compte dissocié continue d'apparaître dans l'inventaire des comptes.
- Le compte GuardDuty administrateur n'a plus accès aux résultats de ce compte autonome.
- Le titulaire du compte n'est pas informé de la dissociation.

Vous pourrez ajouter à nouveau le compte dissocié à votre organisation ultérieurement.

Choisissez une méthode préférée pour dissocier (supprimer) un compte membre de votre organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte d' GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

3. Dans le tableau des comptes, vous pouvez supprimer un compte dont le type est Via Organizations et le statut est activé.

Sélectionnez un ou plusieurs comptes ayant le même type et le même statut.

4. Dans le menu déroulant Actions, choisissez Dissocier le compte.
5. Choisissez Dissocier le compte pour confirmer votre sélection.
6. La valeur du statut des comptes sélectionnés deviendra Non membre. Le nombre de Via Organizations (Active/All) dans le coin supérieur droit de la page des comptes changera pour refléter la mise à jour.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez dissocier le compte membre.

API

1. Pour récupérer l'identifiant du compte membre que vous souhaitez supprimer, utilisez l'[ListMembers](#) API. Incluez le `OnlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur `true`, GuardDuty renvoie un `members` tableau fournissant des détails uniquement sur les comptes actuellement GuardDuty membres.

Vous pouvez également utiliser AWS Command Line Interface (AWS CLI) pour exécuter la commande suivante :

```
aws guardduty list-members --only-associated true --region us-east-1
```

Remplacez *us-east-1* par la région dans laquelle vous souhaitez supprimer ce compte.

2. Pour supprimer un ou plusieurs comptes de GuardDuty membre, exécutez [DisassociateMembers](#) la procédure de suppression du compte de membre associé au compte d'administrateur.

Vous pouvez également AWS CLI exécuter la commande suivante :

```
aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE  
--account-ids 111122223333 --region us-east-1
```

Remplacez *us-east-1* par la région dans laquelle vous souhaitez supprimer ce compte. Si vous avez une liste d'identifiants de compte que vous souhaitez supprimer, séparez-les par un espace.

Supprimer des comptes de membres de GuardDuty l'organisation

En tant que compte d' GuardDuty administrateur délégué, une fois que vous avez dissocié un compte de membre et que vous ne souhaitez plus conserver ce compte de membre dans l' GuardDuty organisation, vous pouvez le supprimer de votre GuardDuty organisation. Ce compte de membre n'apparaîtra plus dans l'inventaire de votre compte. Toutefois, s'il n' GuardDuty a pas été suspendu dans ce compte membre, la configuration GuardDuty et les plans de protection dédiés restent les mêmes. Ce compte deviendra désormais un compte autonome et pourra GuardDuty se [désactiver automatiquement](#).

Cette étape ne supprimera pas le compte membre de votre AWS organisation.

Choisissez une méthode préférée pour supprimer un compte membre de votre GuardDuty organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte d' GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Dans le tableau Comptes, vous pouvez supprimer un compte dont le type est Via Organizations et le statut est Supprimé (dissocié).

Sélectionnez un ou plusieurs comptes ayant le même type et le même statut.

4. Dans le menu déroulant Actions, choisissez Supprimer le compte.
5. Choisissez Supprimer les comptes pour confirmer votre sélection. Le membre du compte sélectionné n'apparaîtra plus dans votre tableau des comptes.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez supprimer ce compte de membre.

API/CLI

1. Pour récupérer l'identifiant du compte membre que vous souhaitez supprimer, utilisez l'[ListMembers](#) API. Incluez le `OnlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur `false`, GuardDuty renvoie un `members` tableau qui fournit des détails uniquement sur les comptes actuellement dissociés des GuardDuty membres.

Vous pouvez également utiliser AWS Command Line Interface (AWS CLI) pour exécuter la commande suivante :

```
aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
```

12abc34d567e8fa901bc2d34EXAMPLE Remplacez-le par l'ID du détecteur de compte GuardDuty administrateur délégué et *us-east-1* par la région dans laquelle vous souhaitez supprimer ce compte.

2. Pour supprimer un ou plusieurs comptes GuardDuty membres, exécutez cette [DeleteMembers](#) opération pour supprimer le compte membre de l' GuardDuty organisation.

Vous pouvez également AWS CLI exécuter la commande suivante :

```
aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

12abc34d567e8fa901bc2d34EXAMPLE Remplacez-le par l'identifiant du détecteur de compte GuardDuty administrateur délégué et *us-east-1* par la région dans laquelle vous souhaitez supprimer ce compte. Si vous avez une liste d'identifiants de compte que vous souhaitez supprimer, séparez-les par un espace.

Modification du compte GuardDuty d'administrateur délégué

Vous pouvez supprimer le compte d' GuardDuty administrateur délégué de votre organisation dans chaque région, puis déléguer un nouvel administrateur dans chaque région. Pour maintenir le niveau de sécurité des comptes des membres de votre organisation dans une région, vous devez disposer d'un compte d' GuardDuty administrateur délégué dans cette région.

 Remarque

Avant de supprimer un compte d' GuardDuty administrateur délégué, vous devez dissocier tous les comptes de membres associés au compte d' GuardDuty administrateur délégué, puis les supprimer de l' GuardDuty organisation. Pour plus d'informations sur ces étapes, consultez les documents suivants :

- [Dissociation \(suppression\) du compte membre du compte administrateur](#)
- [Supprimer des comptes de membres de GuardDuty l'organisation](#)

Supprimer un compte d' GuardDuty administrateur délégué existant

Étape 1 - Pour supprimer le compte d' GuardDuty administrateur délégué existant dans chaque région

1. En tant que compte d' GuardDuty administrateur délégué existant, listez tous les comptes de membre associés à votre compte d'administrateur. Courez [ListMembers](#) avec `OnlyAssociated=false`.
2. Si la préférence d'activation automatique pour GuardDuty ou l'un des plans de protection facultatifs est définie sur ALL, exécutez pour mettre à jour la configuration [UpdateOrganizationConfiguration](#) de l'organisation vers l'un NEW ou NONE l'autre. Cette action empêchera une erreur lorsque vous dissocierez tous les comptes des membres à l'étape suivante.
3. Exécutez [DisassociateMembers](#) pour dissocier tous les comptes de membre associés au compte d'administrateur.
4. Exécutez [DeleteMembers](#) pour supprimer les associations entre le compte administrateur et les comptes membres.
5. En tant que compte de gestion de l'organisation, exécutez la procédure [DisableOrganizationAdminAccount](#) pour supprimer le compte GuardDuty administrateur délégué existant.
6. Répétez ces étapes dans chaque Région AWS cas où vous possédez ce compte GuardDuty d'administrateur délégué.

Étape 2 - Pour désenregistrer le compte GuardDuty administrateur délégué existant dans AWS Organizations (action One-time mondiale)

- Exécutez-le [DeregisterDelegatedAdministrator](#) dans la référence AWS Organizations d'API, pour désenregistrer le compte d' GuardDuty administrateur délégué existant dans AWS Organizations.

Vous pouvez également exécuter la AWS CLI commande suivante :

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --service-principal guardduty.amazonaws.com
```

Assurez-vous de le remplacer **111122223333** par le compte d' GuardDuty administrateur délégué existant.

Après avoir désenregistré l'ancien compte d' GuardDuty administrateur délégué, vous pouvez l'ajouter en tant que compte de membre au nouveau compte d' GuardDuty administrateur délégué.

Désignation d'un nouveau compte d' GuardDuty administrateur délégué dans chaque région

- Désignez un nouveau compte d' GuardDuty administrateur délégué dans chaque région en utilisant votre méthode d'accès préférée (GuardDuty console, API ou AWS CLI. Pour plus d'informations, consultez [Désignation d'un compte d'administrateur délégué GuardDuty](#).
- Exécutez [DescribeOrganizationConfiguration](#) pour afficher la configuration d'activation automatique actuelle de votre organisation.

Important

Avant d'ajouter des membres au nouveau compte d' GuardDuty administrateur délégué, vous devez vérifier la configuration d'activation automatique pour votre organisation. Cette configuration est spécifique au nouveau compte d' GuardDuty administrateur délégué et à la région sélectionnée, et n'est pas liée à AWS Organizations. Lorsque vous ajoutez un compte de membre de l'organisation (nouveau ou existant) sous le nouveau compte d' GuardDuty administrateur délégué, la configuration d'activation automatique

du nouveau compte d' GuardDuty administrateur délégué s'applique au moment de l'activation GuardDuty ou de l'un de ses plans de protection facultatifs.

Modifiez la configuration de l'organisation pour le nouveau compte d' GuardDuty administrateur délégué en utilisant votre méthode d'accès préférée (GuardDuty console, API ou AWS CLI. Pour plus d'informations, consultez [Configuration des préférences d'activation automatique de l'organisation](#).

Gestion des comptes à l'aide des politiques de l'organisation

Une politique d' GuardDuty entreprise vous permet d'activer et de gérer Amazon de manière centralisée pour GuardDuty tous les comptes de votre organisation. Vous utilisez une politique AWS Organizations déclarative pour spécifier les entités organisationnelles (racine de l'organisation, unités organisationnelles ou comptes individuels) pour lesquelles le détecteur de GuardDuty base et ses plans de protection sont automatiquement activés et gérés via le compte d' GuardDuty administrateur délégué. Les comptes qui rejoignent l'organisation ou migrent vers une unité d'organisation à laquelle est attachée une politique héritent de cette politique et leurs plans de protection sont GuardDuty configurés conformément à ce que la politique effective définit pour eux.

GuardDuty les politiques de l'organisation constituent un mécanisme différent des paramètres d'activation automatique décrits dans [Gérer des GuardDuty comptes avec AWS Organizations](#). Pour le concept, la structure, l'héritage, la validation et les exemples de politiques, voir [GuardDutyles politiques](#) dans le guide de AWS Organizations l'utilisateur.

Table des matières

- [Conditions préalables](#)
- [Comment fonctionnent les politiques de l'organisation](#)
- [Création d'une politique dans la console](#)
- [Examiner l'impact d'une politique avant de l'appliquer](#)
- [Considérations et restrictions](#)

Conditions préalables

Avant d'utiliser les politiques de GuardDuty l'organisation, remplissez les conditions préalables suivantes :

- Activez un accès sécurisé pour le GuardDuty service dans AWS Organizations.
- Attribuez un compte GuardDuty d'administrateur délégué.
- Joignez la politique de délégation qui accorde à l'administrateur délégué l'autorisation de gérer GuardDuty les politiques.
- Activez le type de politique GUARDDUTY_POLICY à la racine de l'organisation. Cela se produit automatiquement lorsque l'administrateur délégué crée la première politique dans la GuardDuty console.

Warning

L'activation du type de GUARDDUTY_POLICY stratégie empêche les paramètres GuardDuty d'activation automatique régionaux de s'appliquer, même avant que vous n'associiez une politique. Comme la console active automatiquement ce type de stratégie lorsque l'administrateur délégué crée la première stratégie, vous pouvez arrêter de vous fier à l'activation automatique sans en avoir l'intention. Passez en revue votre configuration d'activation automatique existante avant de créer votre première politique.

Pour les étapes détaillées, consultez [GuardDutyles politiques](#) dans le guide de AWS Organizations l'utilisateur.

Comment fonctionnent les politiques de l'organisation

Une politique d' GuardDuty entreprise détermine quelles GuardDuty fonctionnalités sont activées, dans quelles régions et pour quels comptes. Les sections suivantes décrivent comment une politique s'applique à toutes les régions, comment les politiques sont héritées au sein de votre organisation, comment une politique active modifie la façon dont vous gérez les GuardDuty comptes et les méthodes courantes d'utilisation d'une politique.

Table des matières

- [Configuration régionale](#)
- [Héritage et priorité des politiques](#)
- [Comment une politique affecte la gestion des GuardDuty comptes](#)
- [Exemples de cas d'utilisation](#)

Configuration régionale

Une politique GuardDuty organisationnelle définit l'activation par région. La configuration par défaut s'applique à toutes les régions où GuardDuty elle est disponible. Vous pouvez ajouter une dérogation régionale pour donner une configuration différente à une région spécifique. La configuration par défaut est facultative. Si vous l'omettez, seules les régions que vous spécifiez sont gérées, et toutes les autres régions ne sont pas gérées.

Lorsqu'une politique est activée de GuardDuty manière générale, telle qu'une configuration par défaut qui couvre toutes les régions, elle GuardDuty traite les événements de service AWS CloudTrail globaux dans toutes les régions où elle est activée, y compris les régions où vous n'avez ni ressources ni charge de travail. Pour plus d'informations, consultez [Comment GuardDuty gère AWS CloudTrail événements mondiaux](#).

Une politique gère GuardDuty et un plan de protection uniquement dans les régions où ils sont disponibles. Si votre politique l'autorise GuardDuty ou si un plan de protection n'est pas disponible dans une région où il n'est pas disponible, la politique l'ignore dans cette région sans erreur. Avant de configurer une politique, vérifiez où GuardDuty et où chaque plan de protection est disponible. Pour plus d'informations, consultez [Region-specific disponibilité des fonctionnalités](#).

Une dérogation régionale remplace entièrement la configuration par défaut pour cette région. Il ne fusionne pas avec le plan par défaut. Vous devez donc spécifier tous les plans de protection que vous souhaitez gérer dans cette région. Tout plan de protection que vous omettez lors d'une dérogation n'est pas géré dans cette région, même si la configuration par défaut le gère. De ce fait, les plans de protection gérés par une politique peuvent différer d'une région à l'autre.

Pour connaître la structure complète des politiques et la manière dont les régions sont résolues, voir [GuardDuty les politiques](#) dans le guide de AWS Organizations l'utilisateur.

Héritage et priorité des politiques

GuardDuty les politiques de l'organisation suivent le modèle d' AWS Organizations héritage. Une politique attachée à la racine de l'organisation s'applique à tous les comptes de l'organisation. Les comptes héritent également de toute politique attachée à une unité d'organisation parent. Lorsque plusieurs politiques s'appliquent à un compte, elles sont AWS Organizations fusionnées en une seule politique effective, et une politique attachée plus près du compte a priorité sur une stratégie attachée plus haut dans la hiérarchie.

Une fois que vous avez activé le type de GUARDDUTY_POLICY stratégie, la stratégie a priorité sur les paramètres d' GuardDuty activation automatique régionaux. Les paramètres d'activation automatique ne s'appliquent plus, qu'une politique soit attachée ou non.

Pour connaître l'intégralité des règles d'héritage et la manière dont la politique effective est résolue, voir [Comprendre l'héritage des politiques de gestion](#) dans le Guide de AWS Organizations l'utilisateur.

Comment une politique affecte la gestion des GuardDuty comptes

Lorsqu'une politique d' GuardDuty organisation est active, les modifications suivantes s'appliquent à la façon dont vous gérez les GuardDuty comptes :

- Une fois le type de GUARDDUTY_POLICY stratégie activé, les paramètres GuardDuty d'activation automatique régionaux ne s'appliquent plus, qu'une politique soit attachée ou non.
- Lorsqu'une politique gère un plan de protection, celui-ci ne peut plus être modifié via la GuardDuty console ou l'API des comptes couverts. Sur la page Comptes, il apparaît comme étant géré par des politiques. Pour modifier un plan de protection géré, mettez à jour la politique. Les plans de protection que la politique ne gère pas restent modifiables via la console et l'API.
- Seul le compte d'administrateur délégué peut créer et gérer GuardDuty des politiques. La page Politiques de l'organisation de la GuardDuty console n'est accessible qu'à l'administrateur délégué.

Note

L'ajout d'une GuardDuty politique permet d'inscrire de nouveaux comptes en tant que GuardDuty membres et d'activer des plans de protection au sein de votre organisation. L'activation GuardDuty et ses plans de protection entraînent des frais. Pour plus d'informations, consultez [Tarification en GuardDuty](#).

Exemples de cas d'utilisation

Les exemples suivants montrent les méthodes courantes d'utilisation d'une politique d' GuardDuty entreprise. Pour la politique JSON qui implémente chaque modèle, consultez [GuardDuty les politiques](#) dans le guide de AWS Organizations l'utilisateur.

- Mettez en place une base de protection pour l'ensemble de l'entreprise. Associez une politique à la racine de l'organisation avec une configuration par défaut qui active le détecteur de base et les

plans de protection dont vous avez besoin. Chaque compte, y compris les comptes auxquels il est possible de se connecter ultérieurement, active automatiquement ces fonctionnalités.

- Variez la protection par unité organisationnelle. Utilisez une politique générale à la base de votre base de référence et associez des politiques plus spécifiques aux unités d'organisation individuelles afin d'adapter les plans de protection aux comptes présentant des exigences de conformité ou de charge de travail différentes.
- Maintenez la couverture au fur et à mesure que votre organisation se développe. Étant donné que les comptes qui rejoignent l'organisation ou sont transférés dans une unité d'organisation couverte héritent de la politique en vigueur, une politique permet aux comptes nouvellement créés d'être alignés sur votre base de protection sans activation manuelle.

Création d'une politique dans la console

Vous créez et gérez les GuardDuty politiques à partir du compte d'administrateur délégué, sur la page Politiques d'organisation de la GuardDuty console. La création de votre première politique active également automatiquement le type de GUARDDUTY_POLICY stratégie pour votre organisation.

Pour créer une GuardDuty politique

1. Connectez-vous à la GuardDuty console avec le compte d'administrateur délégué.
2. Dans le volet de navigation, choisissez Politiques d'organisation, puis sélectionnez Créer une politique.
3. Pour Étape 1 : Détails de la politique, entrez un nom de politique et une description facultative, puis choisissez Next.
4. Pour l'étape 2 : Comptes, choisissez l'endroit où la politique est attachée dans la hiérarchie de votre organisation, puis choisissez Suivant :
 - Toutes les unités organisationnelles et tous les comptes associent la politique à l'ensemble de l'organisation.
 - Des unités organisationnelles et des comptes spécifiques l'associent aux entités que vous sélectionnez.
 - Aucune unité organisationnelle ni aucun compte ne crée la politique sans l'associer.
5. Pour l'étape 3 : Détails de configuration, sous Sélection des capacités, sélectionnez les plans de protection gérés par cette politique. Utilisez Activer tout ou Désactiver tout pour commencer rapidement, puis ajustez les plans de protection individuels. Les plans de protection que vous ne

sélectionnez pas ne sont pas concernés par cette politique. La détection des menaces de base doit être activée si vous activez un autre plan de protection. Choisissez Suivant.

6. (Facultatif) Pour l'étape 4 : Dérogations régionales, choisissez Ajouter une dérogation régionale, sélectionnez une ou plusieurs régions et définissez la configuration pour ces régions. Une dérogation régionale remplace entièrement la configuration par défaut de la région. Spécifiez donc tous les plans de protection que vous souhaitez y gérer. Choisissez Suivant.
7. Pour l'étape 5 : révision et création, passez en revue les détails de la politique, les comptes, la configuration par défaut et les éventuelles dérogations régionales. Pour voir le JSON de politique généré, développez le document de politique. Sélectionnez ensuite Créer une politique.

Vous pouvez consulter ou modifier le JSON généré à tout moment en développant le document de politique. Pour la structure des politiques, les règles d'héritage et les exemples de politiques, voir [GuardDuty les politiques](#) dans le Guide de AWS Organizations l'utilisateur.

Examiner l'impact d'une politique avant de l'appliquer

Avant d'enregistrer une modification de politique qui désactive un plan de protection, vérifiez quels sont les comptes et les régions dans lesquels ce plan de protection est actuellement activé, afin de comprendre ce que le changement va désactiver. Comme une GuardDuty politique s'applique par région, vérifiez l'état d'activation actuel par compte et par région.

Warning

Une politique qui le désactive GuardDuty ou un plan de protection le désactive dans tous les comptes couverts où il est actuellement activé et empêche ces comptes de le réactiver via la console ou l'API. Vous pouvez désactiver involontairement la protection sur laquelle les comptes s'appuient. Avant de créer ou de mettre à jour une politique, identifiez les comptes et les régions concernés par le changement, comme décrit dans cette section, et confirmez que l'impact est prévu.

En tant qu'administrateur délégué, vous pouvez consulter l' GuardDuty activation actuelle au sein de votre organisation en utilisant la page des comptes de la GuardDuty console (changez de région pour vérifier la couverture de chaque région) ou par programmation en suivant les étapes suivantes. Effectuez les étapes de l'API dans chaque région que vous souhaitez examiner.

Pour identifier les comptes et les régions concernés par une politique

1. Énumérez les comptes de votre organisation. Utilisez l'opération AWS Organizations `ListAccounts` API pour répertorier tous les comptes de l'organisation, y compris les comptes qui ne sont pas encore GuardDuty membres.
2. Énumérez vos comptes GuardDuty de membres. Utilisez l'opération GuardDuty `ListMembers` API pour répertorier les comptes déjà GuardDuty membres.
3. Passez en revue les plans de protection activés pour chaque compte membre. Utilisez l'opération GuardDuty `GetMemberDetectors` API pour voir quelles fonctionnalités sont activées pour le détecteur de chaque compte membre.
4. Comparez l'activation actuelle aux plans de protection que votre changement de politique désactivera pour identifier les comptes et les régions concernés par le changement.

Un compte qui appartient à votre organisation mais qui n'est pas encore GuardDuty membre n'y apparaît pas `ListMembers`, et vous ne pouvez pas voir son statut de détecteur tant que vous ne l'avez pas ajouté en tant que membre. Lorsqu'une GuardDuty politique s'applique à un compte qui n'est pas encore membre, le compte est automatiquement ajouté en tant que membre.

Après avoir créé et joint une politique, confirmez la politique finale qui s'applique à un compte spécifique. La politique effective est l'agrégation de toutes les politiques que le compte hérite de ses entités mères, combinées à toute politique directement attachée au compte. Pour l'afficher, utilisez l'opération AWS Organizations `DescribeEffectivePolicy` API, ou ses équivalents AWS CLI ou AWS SDK, avec le type de GuardDuty politique. Tout compte autorisé à appeler cette opération peut l'utiliser, y compris le compte d'administrateur délégué. Pour plus d'informations, consultez la section [Affichage des politiques déclaratives efficaces](#) dans le Guide de l' AWS Organizations utilisateur.

Considérations et restrictions

Tenez compte des points suivants lorsque vous planifiez et gérez les politiques de GuardDuty l'organisation :

- Une politique s'applique uniquement aux comptes ouverts AWS Organizations. Une politique d'organisation GuardDuty ne peut être gérée que dans les comptes appartenant à votre organisation via AWS Organizations. Il ne peut pas gérer les comptes qui ne font pas partie de votre organisation, tels que les comptes associés uniquement par l'ancienne méthode d'invitation. Gérez GuardDuty dans ces comptes séparément, à partir du compte GuardDuty administrateur

délégué ou dans chaque compte. Pour plus d'informations sur les deux méthodes d'association, consultez [Gérer plusieurs comptes sur Amazon GuardDuty](#).

- Une politique ne peut être activée GuardDuty dans le compte de gestion que si le rôle lié au service y existe déjà. Une politique ne peut pas être activée GuardDuty dans le compte de gestion de l'organisation à moins que le rôle GuardDuty lié au service n'existe déjà dans ce compte. Si le rôle est absent, GuardDuty il n'est pas activé dans le compte de gestion même lorsque la politique le déclare activé. Créez le rôle dans le compte de gestion, par exemple en l'activant GuardDuty , avant de vous fier à une politique pour le gérer.
- L'administrateur délégué est affecté par région, et l'activation des comptes est indépendante de leur affichage. Le compte de gestion désigne l'administrateur GuardDuty délégué dans chaque région. Un administrateur délégué affecté dans une région peut créer une politique autorisant GuardDuty les comptes de membres, y compris dans les régions où il n'est pas l'administrateur délégué. Toutefois, l'administrateur délégué ne peut pas voir le statut ou les résultats de ces comptes membres dans une région à moins que le compte de gestion ne l'ait également désigné comme administrateur délégué dans cette région. Pour gérer et surveiller les comptes des membres dans une région, le compte de gestion doit désigner l'administrateur délégué de cette région. Comme la désignation se fait par région, le compte de gestion peut désigner différents comptes en tant qu'administrateur délégué dans différentes régions, et chaque administrateur délégué gère et surveille les comptes des membres uniquement dans les régions où il est désigné.
- L'administrateur délégué a besoin de la politique de AWS Organizations délégation pour gérer les politiques. La désignation d'un administrateur délégué lui permet de consulter les comptes des membres, mais il ne peut pas créer, mettre à jour ou joindre des politiques d' GuardDuty organisation à moins que la politique de AWS Organizations délégation ne lui accorde également l'autorisation de gérer le type de GUARDDUTY_POLICY politique. Si ces opérations sont refusées, vérifiez que la politique de délégation accorde à l'administrateur délégué l'autorisation de gérer le type de stratégie.
- Un plan de protection géré est en lecture seule dans la console et dans l'API. Lorsqu'une politique gère un plan de protection, les comptes couverts ne peuvent pas le modifier via la GuardDuty console ou l'API. Pour modifier un plan de protection géré, mettez à jour la politique. Les plans de protection que la politique ne gère pas restent modifiables via la console et l'API.
- Une politique gère uniquement l'activation, et non les personnalisations de détection. Une politique d' GuardDuty entreprise active et désactive GuardDuty ses plans de protection. Il ne gère pas les personnalisations de détection telles que les listes d'entités, les listes d'adresses IP ou les règles de suppression. Configurez-les séparément via la GuardDuty console ou l'API après GuardDuty

leur activation. Pour plus d'informations, consultez [Personnalisation de la détection des menaces à l'aide de listes d'entités et de listes d'adresses IP](#) et [Règles de suppression dans GuardDuty](#).

- Une région non gérée reste inchangée et n'est pas désactivée. Une région qu'une politique n'inclut pas dans la configuration par défaut et dont le nom n'est pas inclus dans une dérogation régionale n'est pas gérée. La politique GuardDuty n'active ni ne désactive cette zone, et les paramètres existants dans cette région restent inchangés.
- GuardDuty traite les événements mondiaux dans chaque région activée. GuardDuty reproduit les événements de service AWS CloudTrail mondiaux, à partir de services tels que IAM AWS STS, Amazon S3 et Amazon CloudFront, et les traite dans toutes les régions où cette option GuardDuty est activée, y compris les régions où vous n'avez aucune ressource ni charge de travail. Cela améliore la détection des menaces, mais cela signifie que lorsqu'une politique l'autorise de manière générale, telle qu'une configuration par défaut couvrant toutes les régions, elle GuardDuty traite ces événements mondiaux dans toutes ces régions, ce qui peut entraîner des GuardDuty coûts supplémentaires. Pour plus d'informations, consultez [Comment GuardDuty gère AWS CloudTrail événements mondiaux](#) et [Tarification en GuardDuty](#).
- La désactivation d'un plan de protection le désactive là où il est actuellement activé. Une politique qui le désactive GuardDuty ou un plan de protection le désactive dans tous les comptes couverts où il est activé et empêche ces comptes de le réactiver via la console ou l'API. Avant de créer ou de mettre à jour une politique, identifiez les comptes et les régions concernés par le changement, comme décrit dans [Examiner l'impact d'une politique avant de l'appliquer](#).
- Les modifications de politique s'appliquent de manière asynchrone. Un changement de politique se propage au sein de votre organisation et est réconcilié au fil du temps, au lieu de prendre effet instantanément. Prévoyez du temps pour qu'une modification s'applique avant de conclure qu'elle n'a pas pris effet.
- Le détachement d'une politique ne le désactive GuardDuty pas. Lorsque vous dissociez une politique d' GuardDuty organisation d'une entité, les autres politiques que l'entité hérite des entités parentes peuvent toujours s'appliquer et continuer à régir la cible. Si aucune politique efficace n'est maintenue après votre détachement GuardDuty et que ses plans de protection restent dans leur état actuel et ne sont pas désactivés. Dans les deux cas, les modifications futures apportées à votre organisation, telles que l'adhésion de nouveaux comptes ou le transfert de comptes existants vers une unité d'organisation, ne sont plus activées GuardDuty automatiquement, sauf si une politique héritée les couvre toujours. Toute activation supplémentaire doit être effectuée manuellement, en rattachant une politique ou par le biais d'une politique héritée.
- La désactivation du type de stratégie arrête toute gestion des politiques et rétablit l'activation automatique. La désactivation GuardDuty dans une politique, le détachement d'une stratégie et la

désactivation du type de GUARDDUTY_POLICY stratégie sont trois actions différentes ayant des effets différents. Lorsque vous désactivez le type de GUARDDUTY_POLICY politique à la racine de l' GuardDutyorganisation, les politiques de l'organisation ne régissent plus aucun compte et GuardDuty restent activées dans les comptes qu'elles couvraient auparavant. La désactivation du type de stratégie rétablit également les paramètres GuardDuty d'activation automatique régionaux que l'activation du type de stratégie avait supprimés, de sorte que l'activation automatique reprend conformément à ces paramètres.

Gestion GuardDuty des comptes sur invitation

Pour gérer des comptes en dehors de votre organisation, vous pouvez utiliser la méthode d'invitation héritée. Lorsque vous utilisez cette méthode, votre compte est désigné comme compte administrateur lorsqu'un autre compte accepte votre invitation à devenir un compte membre.

Note

GuardDuty recommande d'utiliser AWS Organizations plutôt que des GuardDuty invitations pour gérer vos comptes de membres. Pour de plus amples informations, veuillez consulter [Gestion de comptes avec AWS Organizations](#).

Si votre compte n'est pas un compte administrateur, vous pouvez accepter une invitation provenant d'un autre compte. Lorsque vous acceptez, votre compte devient un compte membre. Un AWS compte ne peut pas être à la fois un compte GuardDuty administrateur et un compte membre.

Lorsque vous acceptez l'invitation d'un compte, vous ne pouvez pas accepter l'invitation d'un autre compte. Pour accepter une invitation provenant d'un autre compte, vous devez d'abord dissocier votre compte du compte administrateur existant. Le compte administrateur peut également dissocier votre compte de son organisation et le supprimer.

Les comptes associés par invitation entretiennent la même relation globale entre le compte administrateur et le membre que les comptes associés par AWS Organizations, comme décrit dans [Comprendre la relation entre le compte GuardDuty administrateur et les comptes membres](#). Toutefois, les utilisateurs du compte administrateur des invitations ne peuvent pas GuardDuty activer au nom des comptes membres associés ni consulter d'autres comptes non membres au sein de leur AWS Organizations organisation.

Important

Cross-regional un transfert de données peut avoir lieu lors de la GuardDuty création de comptes membres à l'aide de cette méthode. Afin de vérifier les adresses e-mail des comptes des membres, GuardDuty utilise un service de vérification des e-mails qui fonctionne uniquement dans la région de l'est des États-Unis (Virginie du Nord).

Rubriques

- [Ajouter des comptes sur invitation](#)
- [Consolidation des comptes d' GuardDuty administrateurs au sein d'une seule organisation](#)

Ajouter des comptes sur invitation

En tant que compte administrateur déjà GuardDuty activé, vous pouvez ajouter des membres pour commencer à l'utiliser GuardDuty. Après avoir ajouté les membres, vous pouvez les inviter à vous rejoindre GuardDuty et ils peuvent choisir de répondre à votre invitation.

Note

GuardDuty recommande d'utiliser AWS Organizations plutôt que des GuardDuty invitations pour gérer vos comptes de membres. Pour de plus amples informations, veuillez consulter [Gestion de comptes avec AWS Organizations](#).

Choisissez une méthode d'accès préférée pour ajouter des comptes de GuardDuty membre en tant que compte d' GuardDuty administrateur.

Console

Étape 1 : ajouter un compte

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Choisissez Ajouter des comptes par invitation dans le panneau supérieur.
4. Sur la page Ajouter des comptes membres, sous Entrer les détails du compte, saisissez l'ID d' Compte AWS et l'adresse e-mail associée au compte que vous souhaitez ajouter.

5. Pour ajouter une autre ligne afin de saisir les détails du compte un par un, choisissez Ajouter un autre compte. Vous pouvez également choisir Charger un fichier .csv avec les détails du compte pour ajouter des comptes en bloc.

⚠ Important

La première ligne de votre fichier csv doit contenir l'en-tête, comme illustré dans l'exemple ci-dessous : Account ID,Email. Chaque ligne suivante doit contenir un seul Compte AWS identifiant valide et l'adresse e-mail associée. Le format d'une ligne est valide si elle ne contient qu'un seul ID Compte AWS et l'adresse e-mail associée séparés par une virgule.

Account ID,Email

55555555555, user@example.com

6. Après avoir ajouté tous les détails des comptes, choisissez Suivant. Vous pouvez consulter les comptes récemment ajoutés dans le tableau Comptes. L'état de ces comptes sera Invitation non envoyée. Pour plus d'informations sur l'envoi d'une invitation à un ou plusieurs comptes ajoutés, veuillez consulter [Step 2 - Invite an account](#).

Étape 2 : inviter un compte

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sélectionnez un ou plusieurs comptes que vous souhaitez inviter sur Amazon GuardDuty.
4. Choisissez le menu déroulant Actions, puis choisissez Inviter.
5. Dans la GuardDuty boîte de dialogue Invitation à, entrez un message d'invitation (facultatif).

Si le compte invité n'a pas accès au courrier électronique, cochez la case Envoyer également une notification par e-mail à l'utilisateur root sur celui de l'invité Compte AWS et générer une alerte sur celui de l'invité. Tableau de bord AWS Health

6. Choisissez Send invitation (Envoyer une invitation). Si les invités ont accès à l'adresse e-mail spécifiée, ils peuvent consulter l'invitation en ouvrant la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>

7. Lorsqu'un invité accepte l'invitation, la valeur de la colonne Statut devient Invité. Pour plus d'informations sur l'acceptation d'une invitation, veuillez consulter [Step 3 - Accept an invitation](#).

Étape 3 : accepter une invitation

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.



Important

Vous devez l'activer GuardDuty avant de pouvoir consulter ou accepter une invitation d'adhésion.

2. Procédez comme suit uniquement si vous ne l'avez pas GuardDuty encore activé ; sinon, vous pouvez ignorer cette étape et passer à l'étape suivante.

Si vous ne l'avez pas encore activé GuardDuty, choisissez Get Started sur la GuardDuty page Amazon.

Sur la page Bienvenue dans GuardDuty, choisissez Activer GuardDuty.

3. Après avoir activé GuardDuty votre compte, procédez comme suit pour accepter l'invitation d'adhésion :
 - a. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
 - b. Choisissez Accounts.
 - c. Sur les comptes, assurez-vous de vérifier le propriétaire du compte à partir duquel vous acceptez l'invitation. Activez Accepter pour accepter l'invitation d'adhésion.
4. Une fois que vous avez accepté l'invitation, votre compte devient un compte GuardDuty membre. Le compte dont le propriétaire a envoyé l'invitation devient le compte GuardDuty administrateur. Le compte administrateur saura que vous avez accepté l'invitation. Le tableau des comptes de leur GuardDuty compte sera mis à jour. La valeur de la colonne État correspondant à votre identifiant de compte de membre deviendra Activé. Le titulaire du compte administrateur peut désormais consulter GuardDuty et gérer les configurations du plan de protection pour le compte de votre compte. Le compte administrateur peut également consulter et gérer les GuardDuty résultats générés pour votre compte membre.

API/CLI

Vous pouvez désigner un compte GuardDuty administrateur et créer ou ajouter des comptes GuardDuty membres sur invitation via les opérations de l'API. Exécutez les opérations GuardDuty d'API suivantes afin de désigner le compte administrateur et les comptes membres dans GuardDuty.

Effectuez la procédure suivante en utilisant les informations d'identification du compte Compte AWS que vous souhaitez désigner comme compte GuardDuty administrateur.

Création ou ajout de comptes membres

1. Exécutez l'opération [CreateMembers](#) API en utilisant les informations d'identification du AWS compte GuardDuty activé. Il s'agit du compte que vous souhaitez utiliser comme GuardDuty compte administrateur.

Vous devez spécifier l'identifiant du détecteur du AWS compte actuel ainsi que l'identifiant du compte et l'adresse e-mail des comptes dont vous souhaitez devenir GuardDuty membres. Vous pouvez créer un ou plusieurs membres avec cette opération d'API.

Vous pouvez également utiliser les outils de ligne de AWS commande pour désigner un compte administrateur en exécutant la commande CLI suivante. Assurez-vous d'utiliser vos propres ID de détecteur, ID de compte et adresse e-mail valides.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Exécutez [InviteMembers](#) en utilisant les informations d'identification du AWS compte GuardDuty activé. Il s'agit du compte que vous souhaitez utiliser comme GuardDuty compte administrateur.

Vous devez spécifier l'identifiant du détecteur du AWS compte actuel et les identifiants des comptes dont vous souhaitez devenir GuardDuty membres. Vous pouvez inviter un ou plusieurs membres avec cette opération d'API.

 Note

Vous pouvez également spécifier un message d'invitation en option à l'aide du paramètre de requête message.

Vous pouvez également l'utiliser AWS Command Line Interface pour désigner des comptes membres en exécutant la commande suivante. Assurez-vous d'utiliser vos propres ID de détecteur et ID de compte valides pour les comptes que vous souhaitez inviter.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-ids 111122223333
```

Acceptation d'invitations

Effectuez la procédure suivante en utilisant les informations d'identification de chaque AWS compte que vous souhaitez désigner comme compte GuardDuty membre.

1. Exécutez l'opération [CreateDetector](#) API pour chaque AWS compte qui a été invité à devenir un compte GuardDuty membre et pour lequel vous souhaitez accepter une invitation.

Vous devez spécifier si la ressource du détecteur doit être activée à l'aide du GuardDuty service. Un détecteur doit être créé et activé GuardDuty pour être opérationnel. Vous devez d'abord l'activer GuardDuty avant d'accepter une invitation.

Vous pouvez également le faire en utilisant les outils de ligne de AWS commande à l'aide de la commande CLI suivante.

```
aws guardduty create-detector --enable
```

2. Exécutez l'opération [AcceptAdministratorInvitation](#) API pour chaque AWS compte pour lequel vous souhaitez accepter l'invitation d'adhésion, en utilisant les informations d'identification de ce compte.

Vous devez spécifier l'ID de détecteur de ce AWS compte pour le compte membre, l'ID de compte du compte administrateur qui a envoyé l'invitation et l'ID d'invitation de l'invitation que vous acceptez. Vous trouverez l'ID de compte du compte administrateur dans l'e-mail d'invitation ou en utilisant l'opération [ListInvitations](#) de l'API.

Vous pouvez également accepter une invitation à l'aide des outils de ligne de AWS commande en exécutant la commande CLI suivante. Assurez-vous d'utiliser un ID de détecteur, un ID de compte administrateur et un ID d'invitation valides.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#)API.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
--administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadc5
```

Consolidation des comptes d' GuardDuty administrateurs au sein d'une seule organisation

GuardDuty recommande d'utiliser le service d'association AWS Organizations pour gérer les comptes des membres sous un compte d' GuardDuty administrateur délégué. Vous pouvez utiliser l'exemple de processus décrit ci-dessous pour consolider le compte administrateur et le membre associé sur invitation dans une organisation sous un seul compte d' GuardDuty administrateur GuardDuty délégué.

Note

GuardDuty recommande d'utiliser AWS Organizations plutôt que des GuardDuty invitations pour gérer vos comptes de membres. Pour de plus amples informations, veuillez consulter [Gestion de comptes avec AWS Organizations](#).

Les comptes déjà gérés par un compte d' GuardDuty administrateur délégué ou les comptes de membres actifs associés à un compte d' GuardDuty administrateur délégué ne peuvent pas être ajoutés à un autre compte d' GuardDuty administrateur délégué. Chaque organisation ne peut avoir

qu'un seul compte d' GuardDuty administrateur délégué par région, et chaque compte de membre ne peut avoir qu'un seul compte d' GuardDuty administrateur délégué.

Choisissez une méthode d'accès préférée pour consolider les comptes d' GuardDuty administrateur sous un seul compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte de gestion de l'organisation.

2. Tous les comptes que vous souhaitez gérer GuardDuty doivent faire partie de votre organisation. Pour plus d'informations sur l'ajout d'un compte à votre organisation, voir [Inviter un Compte AWS homme à rejoindre votre organisation](#).
3. Assurez-vous que tous les comptes de membre sont associés au compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué unique. Dissociez tout compte membre toujours associé aux comptes administrateur préexistants.

Les étapes suivantes vous aideront à dissocier les comptes membres du compte administrateur préexistant :

- a. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
 - b. Pour vous connecter, utilisez les informations d'identification du compte administrateur préexistant.
 - c. Dans le panneau de navigation, choisissez Accounts (Comptes).
 - d. Sur la page Comptes, sélectionnez un ou plusieurs comptes que vous souhaitez dissocier du compte administrateur.
 - e. Choisissez Actions, puis Dissocier le compte.
 - f. Choisissez Confirmer pour finaliser l'étape.
4. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

Pour vous connecter, utilisez les informations d'identification du compte de gestion .

5. Dans le panneau de navigation, sélectionnez Settings (Paramètres). Sur la page Paramètres, désignez le compte GuardDuty d'administrateur délégué pour l'organisation.
6. Connectez-vous au compte d' GuardDuty administrateur délégué désigné.

7. Ajoutez des membres de l'organisation. Pour de plus amples informations, veuillez consulter [Gérer des GuardDuty comptes avec AWS Organizations](#).

API/CLI

1. Tous les comptes que vous souhaitez gérer GuardDuty doivent faire partie de votre organisation. Pour plus d'informations sur l'ajout d'un compte à votre organisation, voir [Inviter un Compte AWS homme à rejoindre votre organisation](#).
2. Assurez-vous que tous les comptes de membre sont associés au compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué unique.
 - a. Exécutez [DisassociateMembers](#) pour dissocier tout compte de membre toujours associé aux comptes d'administrateur préexistants.
 - b. Vous pouvez également AWS Command Line Interface exécuter la commande suivante et la **77777777777** remplacer par l'ID de détecteur du compte administrateur préexistant dont vous souhaitez dissocier le compte membre.
66666666666 Remplacez-le par l' Compte AWS ID du compte membre que vous souhaitez dissocier.

```
aws guardduty disassociate-members --detector-id 77777777777 --account-ids 66666666666
```

3. Exécutez [EnableOrganizationAdminAccount](#) pour déléguer un compte Compte AWS en tant GuardDuty qu'administrateur délégué.

Vous pouvez également exécuter la commande suivante AWS Command Line Interface pour déléguer un compte d' GuardDuty administrateur délégué :

```
aws guardduty enable-organization-admin-account --admin-account-id 77777777777
```

4. Ajoutez des membres de l'organisation. Pour de plus amples informations, veuillez consulter [Create or add member member accounts using API](#).

⚠ Important

Pour optimiser l'efficacité d' GuardDutyun service régional, nous vous recommandons de désigner votre compte d' GuardDuty administrateur délégué et d'ajouter tous vos comptes de membre dans chaque région.

GuardDuty considérations relatives à l'exportation des détails du compte d'un membre au format CSV

En tant que compte GuardDuty administrateur, vous pouvez exporter les détails du compte du membre au format CSV. Ces informations incluent l'ID du compte membre, le nom, le type (ajouté par AWS Organizations ou via une invitation), l'état de configuration GuardDuty et les plans de protection dédiés.

L'option Exporter au format CSV s'affiche sur la page GuardDuty Comptes en fonction de la façon dont vous gérez les comptes de plusieurs membres. En utilisant l'option Exporter au format CSV, vous pouvez identifier les comptes membres pour lesquels un plan de protection spécifique est activé.

La liste suivante indique les critères permettant de savoir si le fichier CSV d'exportation sera disponible ou non sur la page de vos GuardDuty comptes :

- Vous ne l'utilisez que AWS Organizations pour gérer plusieurs comptes de membres et le nombre total de comptes de membres dans votre GuardDuty organisation peut atteindre 5 000.
- Vous utilisez à la fois AWS Organizations la méthode des invitations, et le nombre total de comptes membres de votre GuardDuty organisation peut atteindre 5 000.

Dans ce scénario, le fichier CSV exporté indiquera si un compte de membre a été ajouté via AWS Organizations ou en utilisant une méthode basée sur une invitation.

- Lorsque vous utilisez uniquement la méthode basée sur invitation pour gérer plusieurs comptes de membres, il n'existe aucune option Exporter au format CSV.

GuardDuty types de recherche

Une découverte est une notification qui est GuardDuty générée lorsqu'elle détecte une indication d'une activité suspecte ou malveillante dans votre Compte AWS. GuardDuty génère une recherche dans un compte qui a été activé GuardDuty.

Pour plus d'informations sur les modifications importantes apportées aux types de GuardDuty recherche, y compris les types de recherche récemment ajoutés ou retirés, voir [Historique du document pour Amazon GuardDuty](#).

Pour plus d'informations sur les types de résultat désormais retirés, veuillez consulter [Retrait de types de résultat](#).

GuardDuty Types de recherche EC2

Les résultats suivants sont propres aux ressources Amazon EC2 et ont toujours le type de ressource Instance. La gravité et les détails des résultats diffèrent selon le rôle de la ressource, qui indique si la ressource EC2 était la cible ou l'auteur d'une activité suspecte.

Les résultats répertoriés ici incluent les sources de données et les modèles utilisés pour générer ce type de résultat. Pour plus d'informations sur les sources de données et les modèles, veuillez consulter [GuardDuty sources de données de base](#).

Remarques

- Les détails de l'instance de recherche EC2 peuvent être manquants si l'instance a déjà été interrompue ou si l'appel d'API sous-jacent provient d'une instance EC2 d'une autre région.
- Les résultats de l'EC2 qui utilisent les journaux de flux VPC comme source de données ne prennent pas en charge le trafic IPv6.

Pour tous les résultats EC2, il est recommandé d'examiner la ressource en question afin de déterminer si elle se comporte comme prévu. Si l'activité est autorisée, vous pouvez utiliser les listes de règles de suppression ou d'adresses IP approuvées pour éviter les notifications faussement positives pour cette ressource. En cas d'activité inattendue, la bonne pratique en matière de sécurité consiste à supposer que l'instance est compromise et à prendre les mesures détaillées dans [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Rubriques

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [Behavior:EC2/NetworkPortUnusual](#)
- [Behavior:EC2/TrafficVolumeUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Custom](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)
- [Recon:EC2/PortProbeEMRUnprotectedPort](#)
- [Recon:EC2/PortProbeUnprotectedPort](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)

- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/MetadataDNSRebind](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)

Backdoor:EC2/C&CActivity.B

Une instance EC2 interroge une adresse IP associée à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance répertoriée dans votre environnement AWS interroge une adresse IP avec un serveur de commande et de contrôle connu. L'instance répertoriée est peut-être compromise. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui sont infectés et contrôlés par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer une attaque par déni de service distribué (DDoS).

Note

Si l'adresse IP demandée est liée à log4j, les champs du résultat associé incluront les valeurs suivantes :

- service.additional = Amazon Info.threatListName
- service.additional Info.threatName = Lié à Log4j

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/C&CActivity.B!DNS

Une instance EC2 interroge un nom de domaine associé à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance répertoriée dans votre environnement AWS interroge un nom de domaine avec un serveur de commande et de contrôle connu. L'instance répertoriée est peut-être compromise. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui sont infectés et contrôlés par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer une attaque par déni de service distribué (DDoS).

Note

Si le nom de domaine demandé est lié à log4j, les champs du résultat associé incluront les valeurs suivantes :

- `service.additional = Amazon Info.threatListName`
- `service.additional Info.threatName = Lié à Log4j`

Note

Pour tester le GuardDuty mode de génération de ce type de recherche, vous pouvez effectuer une requête DNS depuis votre instance `dig` (sous Linux ou `nslookup` Windows) sur un domaine de `testguardduty2activityb.com`.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/DenialOfService.Dns

Une instance EC2 se comporte d'une manière pouvant indiquer qu'elle est utilisée pour réaliser une attaque Denial of Service (DoS) à l'aide du protocole DNS.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic DNS sortant. Cela peut indiquer que l'instance répertoriée est compromise et utilisée pour réaliser des attaques par déni de service (DoS) à l'aide du protocole DNS.

Note

Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/DenialOfService.Tcp

Une instance EC2 se comporte d'une manière indiquant qu'elle est utilisée pour réaliser une attaque DoS (Denial of Service) à l'aide du protocole TCP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic TCP sortant. Cela peut indiquer que l'instance est compromise et utilisée pour réaliser des attaques par déni de service (DoS) à l'aide du protocole TCP.

Note

Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/DenialOfService.Udp

Une instance EC2 se comporte d'une manière indiquant qu'elle est utilisée pour réaliser une attaque DoS (Denial of Service) à l'aide du protocole UDP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic UDP sortant. Cela peut indiquer que l'instance répertoriée est compromise et utilisée pour réaliser des attaques par déni de service (DoS) à l'aide du protocole UDP.

 Note

Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Une instance EC2 se comporte d'une manière pouvant indiquer qu'elle est utilisée pour réaliser une attaque Denial of Service (DoS) à l'aide du protocole UDP sur un port TCP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic UDP sortant ciblé sur un port qui est généralement utilisé pour les communications TCP. Cela peut indiquer que l'instance répertoriée est compromise et utilisée pour réaliser des attaques par déni de service (DoS) à l'aide du protocole UDP sur un port TCP.

 Note

Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/DenialOfService.UnusualProtocol

Une instance EC2 se comporte d'une manière pouvant indiquer qu'elle est utilisée pour réaliser une attaque Denial of Service (DoS) à l'aide d'un protocole inhabituel.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic sortant d'un type de protocole inhabituel qui n'est généralement pas utilisé par des instances EC2, comme Internet Group Management Protocol. Cela peut indiquer que l'instance est compromise et utilisée pour réaliser des attaques par déni de service (DoS) à l'aide d'un protocole inhabituel. Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/Spambot

Une instance EC2 présente un comportement inhabituel en communiquant avec un hôte distant sur le port 25.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS communique avec un hôte distant sur le port 25. Ce comportement est inhabituel, car cette instance EC2 n'a aucun historique de communication sur le port 25. Ce dernier est généralement utilisé par les serveurs de messagerie pour les communications SMTP. Ce résultat indique que votre instance EC2 est peut être compromise et utilisée dans le cadre d'envoi de courriers indésirables.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Behavior:EC2/NetworkPortUnusual

Une instance EC2 communique avec un hôte distant sur un port serveur inhabituel.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a jamais communiqué sur ce port distant auparavant.

Note

Si l'instance EC2 a communiqué sur le port 389 ou le port 1389, la gravité du résultat associé sera modifiée en Élevée et les champs de recherche incluront la valeur suivante :

- service.additional Info.context = Possibilité de rappel log4j

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Behavior:EC2/TrafficVolumeUnusual

Une instance EC2 génère un volume de trafic réseau inhabituellement élevé à destination d'un hôte distant.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a jamais envoyé un tel volume de trafic vers cet hôte distant auparavant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

CryptoCurrency:EC2/BitcoinTool.B

Une instance EC2 interroge une adresse IP associée à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS interroge une adresse IP associée à une activité liée au Bitcoin ou à une autre cryptomonnaie. Le Bitcoin est une cryptomonnaie et un système de paiement numérique mondiaux pouvant faire l'objet d'échanges contre d'autres devises, produits et services. Le bitcoin est une récompense pour le minage de Bitcoins et est très recherché par les acteurs de la menace.

Recommandations de correction :

Si vous utilisez cette instance EC2 pour exploiter ou gérer de la cryptomonnaie, ou si cette instance est impliquée d'une autre manière dans une activité de blockchain, ce résultat peut être une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur CryptoCurrency:EC2/BitcoinTool.B. Le deuxième critère de filtrage doit être l'ID d'instance de l'instance impliquée dans l'activité de blockchain. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

CryptoCurrency:EC2/BitcoinTool.B!DNS

Une instance EC2 interroge un nom de domaine associé à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS interroge un nom de domaine associé à une activité liée au Bitcoin ou à une autre cryptomonnaie. Le Bitcoin est une cryptomonnaie et un système de paiement numérique mondiaux pouvant faire l'objet d'échanges contre d'autres devises, produits et services. Le bitcoin est une récompense pour le minage de Bitcoins et est très recherché par les acteurs de la menace.

Recommandations de correction :

Si vous utilisez cette instance EC2 pour exploiter ou gérer de la cryptomonnaie, ou si cette instance est impliquée d'une autre manière dans une activité de blockchain, ce résultat peut être une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Le deuxième critère de filtrage doit être l'ID d'instance de l'instance impliquée dans l'activité de blockchain. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

DefenseEvasion:EC2/UnusualDNSResolver

Une instance Amazon EC2 communique avec un résolveur DNS public inhabituel.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance Amazon EC2 répertoriée de votre environnement AWS se comporte différemment du comportement de référence. Cette instance EC2 n'a aucun historique récent de communication avec ce résolveur DNS public. Le champ Unusual du panneau des détails de recherche de la GuardDuty console peut fournir des informations sur le résolveur DNS demandé.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

DefenseEvasion:EC2/UnusualDoHActivity

Une instance Amazon EC2 effectue une communication DNS sur HTTPS (DoH) inhabituelle.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance Amazon EC2 répertoriée au sein de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a aucun historique récent de communications DNS sur HTTPS (DoH) avec ce serveur DoH public. Le champ Inhabituel dans les détails du résultat peut fournir des informations sur le serveur DoH interrogé.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

DefenseEvasion:EC2/UnusualDoTActivity

Une instance Amazon EC2 effectue une communication DNS sur TLS (DoT) inhabituelle.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a aucun historique récent de communications DNS sur TLS (DoT) avec ce serveur DoT public. Le champ Inhabituel dans le volet des détails du résultat peut fournir des informations sur le serveur DoT interrogé.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/AbusedDomainRequest.Reputation

Une instance EC2 interroge un nom de domaine de mauvaise réputation associé à des domaines abusifs connus.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée au sein de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP abusifs connus. Les noms de domaine de premier niveau (TLD) et les noms de domaine de deuxième niveau (2LD) fournissant des enregistrements de sous-domaines gratuits ainsi que les fournisseurs de DNS dynamiques sont des exemples de domaines utilisés de manière abusive. Les acteurs de la menace ont tendance à utiliser ces services pour enregistrer des domaines gratuitement ou à faible coût. Les domaines de mauvaise réputation de cette catégorie peuvent également être des domaines expirés renvoyés à l'adresse IP de stationnement d'un bureau d'enregistrement et peuvent donc ne plus être actifs. Une adresse IP de stationnement est l'endroit où un bureau d'enregistrement dirige le trafic vers des domaines qui n'ont été liés à aucun service. L'instance Amazon EC2 répertoriée peut être compromise, car les acteurs malveillants utilisent couramment ces bureaux d'enregistrement ou ces services pour la distribution de logiciels malveillants et de commande et de contrôle.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/BitcoinDomainRequest.Reputation

Une instance EC2 interroge un nom de domaine de mauvaise réputation associé à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à une activité liée au Bitcoin ou à une autre cryptomonnaie. Le Bitcoin est une cryptomonnaie et un système de paiement numérique mondiaux pouvant faire l'objet d'échanges contre d'autres devises, produits et services. Le bitcoin est une récompense pour le minage de Bitcoins et est très recherché par les acteurs de la menace.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si vous utilisez cette instance EC2 pour exploiter ou gérer de la cryptomonnaie, ou si cette instance est impliquée d'une autre manière dans une activité de blockchain, ce résultat peut représenter une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur `Impact:EC2/BitcoinDomainRequest.Reputation`. Le deuxième critère de filtrage doit être l'ID d'instance de l'instance impliquée dans l'activité de blockchain. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/MaliciousDomainRequest.Reputation

Une instance EC2 interroge un domaine de mauvaise réputation associé à des domaines malveillants connus.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée au sein de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP malveillants connus. Par exemple, les domaines peuvent être associés à une adresse IP de gouffre connue. Les domaines de gouffre sont des domaines qui étaient auparavant contrôlés par un acteur menaçant, et les demandes qui leur sont adressées peuvent indiquer que l'instance est compromise.

Ces domaines peuvent également être corrélés à des campagnes malveillantes ou à des algorithmes de génération de domaines connus.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/MaliciousDomainRequest.Custom

Une instance EC2 interroge un domaine figurant sur une liste d'entités de menaces personnalisée.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous indique que l'instance Amazon EC2 répertoriée dans votre AWS environnement interroge un nom de domaine inclus dans la liste des entités menaçantes que vous avez chargée et activée. Dans GuardDuty, une liste d'entités menaçantes comprend des noms de domaine et des adresses IP malveillants connus. GuardDuty génère des résultats en fonction de l'activité associée à la liste d'entités de menace téléchargée. Vous pouvez consulter le nom de la liste des entités de menace dans les détails de la recherche.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/PortSweep

Une instance EC2 analyse un port sur un grand nombre d'adresses IP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous indique que l'instance EC2 répertoriée dans votre AWS environnement sonde un port sur un grand nombre d'adresses IP routables publiquement. Ce type d'activité est généralement utilisé pour rechercher des hôtes vulnérables à exploiter. Dans le panneau des informations de recherche de votre GuardDuty console, seule l'adresse IP distante la plus récente est affichée

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/SuspiciousDomainRequest.Reputation

Une instance EC2 interroge un nom de domaine de mauvaise réputation qui est suspect par nature en raison de son ancienneté ou de sa faible popularité.

Gravité par défaut : faible

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée dans votre environnement AWS interroge un nom de domaine de mauvaise réputation suspecté d'être malveillant. Nous avons remarqué des caractéristiques de ce domaine qui étaient cohérentes avec les domaines malveillants précédemment observés, mais notre modèle de réputation n'a pas pu les relier définitivement à une menace connue. Ces domaines sont généralement récemment observés ou reçoivent un faible trafic.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Impact:EC2/WinRMBruteForce

Une instance EC2 exécute une attaque sortante par force brute de Windows Remote Management.

Gravité par défaut : faible*

 Note

La gravité de ce résultat est faible si votre instance EC2 était la cible d'une attaque par force brute. La gravité de ce résultat est élevée si votre instance EC2 est utilisée pour procéder à l'attaque par force brute.

- Source de données : journaux de flux VPC

Ce résultat vous indique que l'instance EC2 répertoriée dans votre AWS environnement exécute une attaque par force brute Windows Remote Management (WinRM) visant à accéder au service Windows-based Windows Remote Management sur les systèmes.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Recon:EC2/PortProbeEMRUnprotectedPort

Un port non protégé lié à EMR d'une instance EC2 est en cours d'exploration par un hôte malveillant connu.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous indique qu'un port sensible lié à l'EMR sur l'instance EC2 répertoriée faisant partie d'un cluster de votre AWS environnement n'est pas bloqué par un groupe de sécurité, une liste de contrôle d'accès (ACL) ou un pare-feu sur hôte tel que Linux IPtables. Cette découverte indique également que des scanners connus sur Internet explorent activement ce port. Les ports qui peuvent déclencher ce résultat, tels que le port 8088 (port YARN Web UI) sont susceptibles d'être utilisés pour l'exécution de code à distance.

Recommandations de correction :

Il est recommandé de bloquer l'accès ouvert aux ports sur les clusters à partir d'Internet et de restreindre l'accès uniquement aux adresses IP qui requièrent un accès à ces ports. Pour de plus amples informations, consultez [Groupes de sécurité pour les clusters EMR](#).

Recon:EC2/PortProbeUnprotectedPort

Un port non protégé d'une instance EC2 est en train d'être analysé par un hôte malveillant connu.

Gravité par défaut : faible*

Note

La gravité par défaut de ce résultat est faible. Toutefois, si le port examiné est utilisé par Elasticsearch (9200 ou 9300), le niveau de gravité du résultat est élevé.

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'un port de l'instance EC2 répertoriée de votre environnement AWS n'est pas bloqué par un groupe de sécurité, une liste de contrôle d'accès (ACL) ou un pare-feu sur l'hôte, comme Linux IPTables, et qu'il est en train d'être analysé activement par des analyseurs connus sur Internet.

Si ce port est le port 22 ou 3389 et que vous utilisez ces ports pour vous connecter à votre instance, vous pouvez toujours limiter leur exposition en autorisant uniquement leur accès aux adresses IP de l'espace d'adressage IP de votre réseau d'entreprise. Pour de plus amples informations sur la restriction de l'accès au port 22 sous Linux, consultez [Autorisation du trafic entrant pour vos instances Linux](#). Pour savoir comment restreindre l'accès au port 3389 sous Windows, consultez [Autorisation du trafic entrant pour vos instances Windows](#).

GuardDuty ne génère pas ce résultat pour les ports 443 et 80.

Recommandations de correction :

Dans certains cas, les instances peuvent être intentionnellement exposées, par exemple si elles hébergent des serveurs Web. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur Recon:EC2/PortProbeUnprotectedPort. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui

hébergent ces outils. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Recon:EC2/Portscan

Une instance EC2 balaie les ports sortants vers un hôte distant.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS est impliquée dans une possible attaque par balayage de ports, car elle tente de se connecter à plusieurs ports sur une courte période. L'objectif d'une attaque par balayage de ports consiste à localiser les ports ouverts pour identifier les services exécutés par la machine et son système d'exploitation.

Recommandations de correction :

Ce résultat peut être un faux positif lorsque des applications d'évaluation de vulnérabilité sont déployées sur des instances EC2 dans votre environnement, car ces applications effectuent des analyses de port pour vous alerter à propos de ports ouverts mal configurés. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur Recon:EC2/Portscan. Le second critère de filtre doit correspondre à l'instance ou aux instances qui hébergent ces outils d'évaluation de vulnérabilité. Vous pouvez utiliser l'attribut ID d'image d'instance ou Valeur de balise en fonction des critères identifiables avec les instances qui hébergent ces outils. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/BlackholeTraffic

Une instance EC2 tente de communiquer avec une adresse IP d'un hôte distant qui est un trou noir connu.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous indique que l'instance EC2 répertoriée dans votre AWS environnement est peut-être compromise car elle tente de communiquer avec l'adresse IP d'un trou noir (ou puits). Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire. Une adresse IP de trou noir désigne une machine hôte qui n'est pas en cours d'exécution ou une adresse à laquelle aucun hôte n'a été attribué.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/BlackholeTraffic!DNS

Une instance EC2 interroge le nom d'un domaine qui est redirigé vers l'adresse IP d'un trou noir.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous indique que l'instance EC2 répertoriée dans votre AWS environnement est peut-être compromise car elle interroge un nom de domaine qui est redirigé vers une adresse IP de trou noir. Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/DGADomainRequest.B

Une instance EC2 interroge des domaines générés par des algorithmes. Ces domaines sont couramment utilisés par des programmes malveillants et peuvent constituer une indication d'instance EC2 compromise.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS tente d'interroger des DGA (algorithmes de génération de noms de domaine). Votre instance EC2 pourrait être compromise.

Ces algorithmes servent à générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle. Les serveurs de commande et de contrôle sont des ordinateurs qui émettent des commandes aux membres d'un botnet, qui est un ensemble d'appareils connectés à Internet qui sont infectés et contrôlés par un type courant de programme malveillant. Le grand nombre de points de rendez-vous potentiels rend l'arrêt des botnets difficile, car les ordinateurs infectés tentent de contacter certains de ces noms de domaine chaque jour pour recevoir des mises à jour ou des commandes.

Note

Ce résultat est basé sur une analyse de noms de domaine utilisant une heuristique avancée et peut donc identifier de nouveaux DGA qui ne sont pas présents dans les flux d'intelligence de menaces.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/DGADomainRequest.C!DNS

Une instance EC2 interroge des domaines générés par des algorithmes. Ces domaines sont couramment utilisés par des programmes malveillants et peuvent constituer une indication d'instance EC2 compromise.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS tente d'interroger des DGA (algorithmes de génération de noms de domaine). Votre instance EC2 pourrait être compromise.

Ces algorithmes servent à générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle. Les serveurs de commande et de contrôle sont des ordinateurs qui émettent des commandes aux membres d'un botnet, qui est un ensemble d'appareils connectés à Internet qui sont infectés et contrôlés par un type courant de programme malveillant. Le grand nombre de points de rendez-vous potentiels rend l'arrêt des botnets difficile, car les ordinateurs infectés tentent de contacter certains de ces noms de domaine chaque jour pour recevoir des mises à jour ou des commandes.

Note

Ce résultat est basé sur les domaines DGA connus issus des flux GuardDuty de renseignements sur les menaces.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/DNSDataExfiltration

Une instance EC2 exfiltre des données via des requêtes DNS.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS exécute un programme malveillant qui utilise des requêtes DNS pour transférer des données sortantes. Ce type de transfert de données indique qu'une instance est compromise et peut entraîner l'exfiltration de données. Généralement, le trafic DNS n'est pas bloqué par des pare-feu. Par exemple, un programme malveillant dans une instance EC2 compromise peut encoder des données, (comme votre numéro de carte de crédit) dans une requête DNS et les envoyer à un serveur DNS distant contrôlé par un pirate.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/DriveBySourceTraffic!DNS

Une instance EC2 interroge le nom de domaine d'un hôte distant qui est une source connue d'attaques par Drive-By téléchargement.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS pourrait être compromise, car elle interroge un nom de domaine qui est un hôte distant étant une source connue d'attaques de type « drive-by-download ». Il s'agit de téléchargements involontaires de logiciels d'Internet qui peuvent déclencher l'installation automatique de virus, logiciels espions ou programmes malveillants.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/DropPoint

Une instance EC2 tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement tente de communiquer avec l'adresse IP d'un hôte distant connu pour détenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/DropPoint!DNS

Une instance EC2 interroge le nom de domaine d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement interroge le nom de domaine d'un hôte distant connu pour contenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Trojan:EC2/PhishingDomainRequest!DNS

Une instance EC2 interroge des domaines impliqués dans des attaques d'hameçonnage. Votre instance EC2 pourrait être compromise.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS tente d'interroger un domaine impliqué dans des attaques de hameçonnage. Les domaines de hameçonnage sont créés par des pirates se faisant passer pour une institution légitime afin de pousser des utilisateurs à fournir des données sensibles, telles que des informations personnelles identifiables, des coordonnées bancaires, des informations de carte bancaire ou des mots de passe. Votre instance EC2 essaie peut-être de récupérer des données sensibles stockées sur un site Web d'hameçonnage ou d'en configurer un. Votre instance EC2 pourrait être compromise.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Une instance EC2 établit des connexions à une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement communique avec une adresse IP figurant sur une liste de menaces que vous avez téléchargée. Dans GuardDuty, une liste de menaces comporte des adresses IP malveillantes connues. GuardDuty génère des résultats en fonction des listes de menaces chargées. La liste de menaces utilisée pour générer ce résultat sera répertoriée dans les détails du résultat.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

UnauthorizedAccess:EC2/MetadataDNSRebind

Une instance EC2 effectue des recherches DNS résolues en service de métadonnées d'instance.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement interroge un domaine qui correspond à l'adresse IP des métadonnées EC2 (169.254.169.254). Une requête DNS de ce type peut indiquer que l'instance est une cible d'une technique de liaison DNS. Celle-ci qui peut être utilisée pour obtenir des métadonnées à partir d'une instance EC2, y compris les informations d'identification IAM associées à l'instance.

La liaison DNS implique de tromper une application s'exécutant sur l'instance EC2 pour charger des données de retour à partir d'une URL, où le nom de domaine de l'URL se résout en adresse IP des métadonnées EC2 (169.254.169.254). Cela conduit l'application à accéder aux métadonnées EC2 et éventuellement à les mettre à la disposition du pirate.

Il est possible d'accéder aux métadonnées EC2 à l'aide de la fonction de liaison DNS uniquement si l'instance EC2 exécute une application vulnérable qui permet l'injection d'URL, ou si une personne accède à l'URL dans un navigateur Web s'exécutant sur l'instance EC2.

Recommandations de correction :

En réponse à ce résultat, vous devez évaluer s'il existe une application vulnérable en cours d'exécution sur l'instance EC2 ou si une personne a utilisé un navigateur pour accéder au domaine identifié dans le résultat. Si la cause première est une application vulnérable, vous devez corriger la vulnérabilité. Si une personne a navigué dans le domaine identifié, vous devez bloquer le domaine ou empêcher les utilisateurs d'y accéder. Si vous déterminez que ce résultat était lié à l'un ou l'autre des cas ci-dessus, [révoquez la session associée à l'instance EC2](#).

Certains AWS clients associent intentionnellement l'adresse IP des métadonnées à un nom de domaine sur leurs serveurs DNS officiels. Si c'est le cas dans votre environnement, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression

doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur UnauthorizedAccess:EC2/MetaDataDNSRebind. Le deuxième critère de filtrage doit être le DNS request domain (Domaine de demande DNS) et la valeur doit correspondre au domaine que vous avez mappé sur l'adresse IP des métadonnées (169.254.169.254). Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

UnauthorizedAccess:EC2/RDPBruteForce

Une instance EC2 a été impliquée dans des attaques en force RDP.

Gravité par défaut : faible*

Note

La gravité de ce résultat est faible si votre instance EC2 était la cible d'une attaque par force brute. La gravité de ce résultat est élevée si votre instance EC2 est utilisée pour procéder à l'attaque par force brute.

- Source de données : journaux de flux VPC

Cette découverte vous indique qu'une instance EC2 de votre AWS environnement a été impliquée dans une attaque par force brute visant à obtenir les mots de passe des services RDP sur les Windows-based systèmes. Cela peut être signe d'un accès non autorisé à vos ressources AWS.

Recommandations de correction :

Si le rôle de ressource de votre instance est ACTOR, cela indique que votre instance a été utilisée pour procéder à des attaques par force brute RDP. À moins que cette instance ait une raison légitime de contacter l'adresse IP répertoriée en tant que Target, il est recommandé de supposer que votre instance est compromise et de prendre les mesures répertoriées dans [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Si le rôle de ressource de votre instance est TARGET, ce résultat peut être corrigé en sécurisant votre port RDP uniquement pour des adresses IP approuvées via des groupes de sécurité, des listes de contrôle d'accès ou des pare-feu. Pour plus d'informations, veuillez consulter [Conseils pour sécuriser vos instances EC2 \(Linux\)](#) (langue française non garantie).

UnauthorizedAccess:EC2/SSHBruteForce

Une instance EC2 a été impliquée dans des attaques en force SSH.

Gravité par défaut : faible*

Note

La gravité de ce résultat est faible si une attaque par force brute vise l'une de vos instances EC2. La gravité de ce résultat est élevée si votre instance EC2 est utilisée pour effectuer l'attaque par force brute.

- Source de données : journaux de flux VPC

Cette découverte vous indique qu'une instance EC2 de votre AWS environnement a été impliquée dans une attaque par force brute visant à obtenir les mots de passe des services SSH sur les Linux-based systèmes. Cela peut être signe d'un accès non autorisé à vos ressources AWS .

Note

Ce résultat est généré uniquement par la surveillance du trafic de sur le port 22. Si vos services SSH sont configurées de façon à utiliser d'autres ports, ce résultat n'est pas généré.

Recommandations de correction :

Si la cible de la tentative de force brute est un hôte bastion, cela peut représenter le comportement attendu de votre AWS environnement. Dans ce cas, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur UnauthorizedAccess:EC2/SSHBruteForce. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si cette activité n'est pas attendue pour votre environnement et que le rôle de ressource de votre instance est TARGET, ce résultat peut être corrigé en sécurisant votre port SSH uniquement pour

des adresses IP approuvées via des groupes de sécurité, des listes de contrôle d'accès ou des pare-feu. Pour plus d'informations, veuillez consulter [Conseils pour sécuriser vos instances EC2 \(Linux\)](#) (langue française non garantie).

Si le rôle de ressource de votre instance est ACTOR, cela indique que l'instance a été utilisée pour procéder à des attaques par force brute SSH. À moins que cette instance ait une raison légitime de contacter l'adresse IP répertoriée en tant que Target, il est recommandé de supposer que votre instance est compromise et de prendre les mesures répertoriées dans [Remédier à une instance Amazon EC2 potentiellement compromise](#).

UnauthorizedAccess:EC2/TorClient

Votre instance EC2 est en train de se connecter à un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Cette découverte vous indique qu'une instance EC2 de votre AWS environnement établit des connexions à un nœud Tor Guard ou Authority. Tor est un logiciel permettant d'activer les communications anonymes. Les nœuds Tor Guards et Authority agissent en tant que passerelles initiales dans un réseau Tor. Ce trafic peut indiquer que cette instance EC2 a été compromise et agit en tant que client sur un réseau Tor. Cette découverte peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

UnauthorizedAccess:EC2/TorRelay

Votre instance EC2 est en train de se connecter à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement établit des connexions à un réseau Tor d'une manière qui suggère qu'elle agit comme un relais Tor. Tor est un logiciel

permettant d'activer les communications anonymes. Tor augmente l'anonymat de la communication en réacheminant le trafic potentiellement illicite du client d'un relais Tor à un autre.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

GuardDuty Types de recherche IAM

Les résultats suivants, spécifiques aux entités IAM et aux clés d'accès, ont toujours un type de ressource de AccessKey. La gravité et les détails des résultats diffèrent selon le type de résultat.

Les résultats répertoriés ici incluent les sources de données et les modèles utilisés pour générer ce type de résultat. Pour plus d'informations, consultez [GuardDuty sources de données de base](#).

Pour tous les IAM-related résultats, nous vous recommandons d'examiner l'entité en question et de vous assurer que ses autorisations respectent les meilleures pratiques du moindre privilège. Si cette activité est inattendue, les informations d'identification peuvent être compromises. Pour plus d'informations sur la correction des résultats, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Rubriques

- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/CompromisedCredentials](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)
- [Discovery:IAMUser/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [PenTest:IAMUser/KaliLinux](#)
- [PenTest:IAMUser/ParrotLinux](#)
- [PenTest:IAMUser/PentoolLinux](#)
- [Persistence:IAMUser/AnomalousBehavior](#)

- [Policy:IAMUser/RootCredentialUsage](#)
- [Policy:IAMUser/ShortTermRootCredentialUsage](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Recon:IAMUser/MaliciousIPCaller](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS](#)
- [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)

CredentialAccess:IAMUser/AnomalousBehavior

Une API utilisée pour accéder à un AWS l'environnement a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule [identité d'utilisateur](#). L'API observée est généralement associée à la phase d'accès aux informations d'identification d'une attaque lorsqu'un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre environnement. Les API de cette catégorie sont GetPasswordDataGetSecretValue, BatchGetSecretValue, etGenerateDbAuthToken.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

CredentialAccess:IAMUser/CompromisedCredentials

Une clé d'accès IAM a été identifiée comme potentiellement compromise par le renseignement sur les menaces Amazon.

Gravité par défaut : élevée

- Fonctionnalité : Inclus dans la protection fondamentale des sources de données

Description complète :

Cette découverte vous indique qu'une clé d'accès IAM associée à votre AWS compte a été identifiée comme potentiellement compromise par Amazon Threat Intelligence. Les informations d'identification compromises ont ensuite été utilisées pour appeler les opérations d'API dans votre AWS environnement. La liste des appels d'API effectués à l'aide des informations d'identification compromises, ainsi que le nombre et l'horodatage de chaque appel, la clé d'accès impliquée et l'adresse IP source sont inclus dans les détails du résultat.

La compromission des informations d'identification dans cette découverte est identifiée par les renseignements sur les menaces d'Amazon. AWS surveille les informations d'identification potentiellement compromises par le biais de modèles d'utilisation et génère ce résultat lorsqu'une telle identification est observée en cours d'utilisation.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

DefenseEvasion:IAMUser/AnomalousBehavior

Une API utilisée pour contourner les mesures défensives a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de couvrir ses traces et d'éviter d'être détecté. Les API de cette catégorie sont généralement des opérations de suppression, de désactivation ou d'arrêt, telles que DeleteFlowLogs, DisableAlarmActions ou StopLogging.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

DefenseEvasion:IAMUser/BedrockLoggingDisabled

La journalisation pour Amazon Bedrock a été désactivée.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que la journalisation a été désactivée pour les invocations du modèle Bedrock dans votre compte. Il peut s'agir d'une tentative d'un attaquant de masquer des activités malveillantes telles que l'exfiltration de données ou l'utilisation abusive de modèles d'IA. La désactivation de la journalisation supprime la visibilité des données envoyées aux modèles et de la manière dont les modèles sont utilisés.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Discovery:IAMUser/AnomalousBehavior

Une API couramment utilisée pour découvrir des ressources a été invoquée de manière anormale.

Gravité par défaut : faible

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à la phase de découverte d'une attaque lorsqu'un adversaire collecte des informations pour déterminer si votre AWS environnement est vulnérable à une attaque de plus grande envergure. Les API de cette catégorie sont généralement des opérations d'obtention, de description ou de liste, telles que DescribeInstances, GetRolePolicy ou ListAccessKeys.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Exfiltration:IAMUser/AnomalousBehavior

Une API couramment utilisée pour collecter des données à partir d'un AWS l'environnement a été invoqué de manière anormale.

Gravité par défaut : élevée

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à des tactiques d'exfiltration dans le cadre desquelles un adversaire tente de collecter des données sur votre réseau en utilisant l'empaquetage et le chiffrement pour éviter d'être détecté. Les API pour ce type de résultat sont uniquement des opérations de gestion (plan de contrôle) et sont généralement liées à S3, aux instantanés et aux bases de données, telles que, PutBucketReplication, CreateSnapshot ou RestoreDBInstanceFromDBSnapshot.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Impact:IAMUser/AnomalousBehavior

Une API couramment utilisée pour altérer des données ou des processus dans un AWS l'environnement a été invoqué de manière anormale.

Gravité par défaut : élevée

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à des tactiques d'impact où un adversaire tente de perturber les opérations et de manipuler, d'interrompre ou de détruire les données de votre compte. Les API pour ce type de résultat sont généralement des opérations de suppression, de mise à jour ou de saisie, telles que DeleteSecurityGroup, UpdateUser ou PutBucketPolicy.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

InitialAccess:IAMUser/AnomalousBehavior

Une API couramment utilisée pour obtenir un accès non autorisé à un AWS l'environnement a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à la phase d'accès initiale d'une attaque lorsqu'un adversaire tente d'accéder à votre environnement. Les API de cette catégorie sont généralement des opérations get token ou de session, telles que `StartSession`, ou `GetAuthorizationToken`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PenTest:IAMUser/KaliLinux

Une API a été invoquée depuis une machine Kali Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une machine exécutant Kali Linux effectue des appels d'API en utilisant des informations d'identification appartenant au AWS compte répertorié dans votre environnement. Kali Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PenTest:IAMUser/ParrotLinux

Une API a été invoquée par une machine Parrot Security Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une machine exécutant Parrot Security Linux effectue des appels d'API en utilisant des informations d'identification appartenant au AWS compte répertorié dans votre environnement. Parrot Security Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PenTest:IAMUser/PentooLinux

Une API a été invoquée par une machine Pentoo Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Cette découverte vous indique qu'une machine exécutant Pentoo Linux effectue des appels d'API en utilisant des informations d'identification appartenant au AWS compte répertorié dans votre environnement. Pentoo Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Persistence:IAMUser/AnomalousBehavior

Une API couramment utilisée pour maintenir un accès non autorisé à un AWS l'environnement a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre environnement et tente de le conserver. Les API de cette catégorie sont généralement des opérations de création, d'importation ou de modification, telles que `CreateAccessKey`, `ImportKeyPair` ou `ModifyInstanceAttribute`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Policy:IAMUser/RootCredentialUsage

Une API a été invoquée à l'aide d'informations d'identification de connexion de l'utilisateur root.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion ou événements de CloudTrail données pour S3

Ce résultat vous informe que les informations d'identification de connexion de l'utilisateur root de l'Compte AWS répertorié dans votre environnement sont utilisées pour effectuer des demandes aux services AWS . Il est recommandé aux utilisateurs de ne jamais utiliser les informations de connexion de l'utilisateur root pour accéder aux AWS services. Les AWS services doivent plutôt être accessibles en utilisant les informations d'identification temporaires AWS Security Token Service (STS) dotées du moindre privilège. Lorsqu' AWS STS n'est pas pris en charge, il est recommandé d'utiliser les informations d'identification d'utilisateur IAM. Pour de plus amples informations, consultez [Bonnes pratiques IAM](#).

Note

Si la protection S3 est activée pour le compte, ce résultat peut être généré en réponse aux tentatives d'exécution des opérations du plan de données S3 sur les ressources Amazon S3 en utilisant les informations de connexion de l'utilisateur root du Compte AWS. L'appel d'API utilisé est répertorié dans les détails d'un résultat. Si la protection S3 n'est pas activée, cette découverte ne peut être déclenchée que par les API du journal des événements. Pour plus d'informations sur S3 Protection, consultez [Protection S3](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Policy:IAMUser/ShortTermRootCredentialUsage

Une API a été appelée à l'aide d'informations d'identification de l'utilisateur racine restreintes.

Gravité par défaut : faible

- Source de données : événements AWS CloudTrail de gestion ou événements de AWS CloudTrail données pour S3

Ce résultat vous indique que les informations d'identification utilisateur restreintes créées pour les utilisateurs répertoriés Compte AWS dans votre environnement sont utilisées pour envoyer des demandes à Services AWS. Il est recommandé d'utiliser les informations d'identification de l'utilisateur root uniquement pour les [tâches qui nécessitent des informations d'identification de l'utilisateur root](#).

Dans la mesure du possible, accédez aux Services AWS rôles IAM avec le moindre privilège avec des informations d'identification temporaires provenant de AWS Security Token Service (AWS STS). Pour les scénarios non AWS STS pris en charge, la meilleure pratique consiste à utiliser les informations d'identification de l'utilisateur IAM. Pour plus d'informations, consultez les [meilleures pratiques de sécurité dans IAM](#) et les [meilleures pratiques pour les utilisateurs root Compte AWS dans le guide](#) de l'utilisateur IAM.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PrivilegeEscalation:IAMUser/AnomalousBehavior

Une API couramment utilisée pour obtenir des autorisations de haut niveau sur un AWS l'environnement a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes faites à proximité par une [identité utilisateur](#) unique. L'API observée est généralement associée à des tactiques d'escalade des privilèges dans le cadre desquelles un adversaire tente d'obtenir des autorisations de niveau supérieur sur un environnement. Les API de cette catégorie impliquent généralement des opérations qui modifient les rôles, les utilisateurs et les politiques IAM, telles que `AssociateIamInstanceProfile`, `AddUserToGroup` ou `PutUserPolicy`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les [détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Recon:IAMUser/MaliciousIPCaller

Une API a été invoquée depuis une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API qui peut répertorier ou décrire vos ressources AWS dans un compte au sein de votre environnement a été appelée depuis une adresse IP figurant sur une liste de menaces. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Recon:IAMUser/MaliciousIPCaller.Custom

Une API a été invoquée depuis une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API qui peut répertorier ou décrire vos ressources AWS dans un compte au sein de votre environnement a été appelée depuis une adresse IP figurant sur une liste de menaces personnalisées. La liste de menaces utilisée sera répertoriée dans les détails du résultat. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Recon:IAMUser/TorIPCaller

Une API a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API qui peut répertorier ou décrire vos ressources AWS dans un compte au sein de votre environnement a été invoquée depuis une adresse IP du nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Un attaquant utiliserait Tor pour masquer sa véritable identité.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail la journalisation a été désactivée.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'un CloudTrail sentier de votre AWS environnement a été désactivé. Il peut s'agir d'une tentative de la part d'un pirate de désactiver la journalisation pour éliminer toute trace de leur activité tout en accédant à vos ressources AWS à des fins malveillantes. Ce résultat peut également être déclenché par une suppression ou une mise à jour réussie d'un journal de suivi. Ce résultat peut également être déclenché par la suppression réussie d'un compartiment S3 qui stocke les journaux d'un journal associé à GuardDuty.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Stealth:IAMUser/PasswordPolicyChange

La stratégie de mot de passe du compte a été affaiblie.

Gravité par défaut : faible*

Note

La gravité de ce résultat peut être faible, moyenne ou élevée en fonction de la gravité des modifications apportées à la stratégie de mot de passe.

- Source de données : événements CloudTrail de gestion

La politique de mot de passe du AWS compte a été affaiblie sur le compte répertorié dans votre AWS environnement. Par exemple, elle a été supprimée ou mise à jour pour exiger moins de caractères ou prolonger la période d'expiration des mots de passe ou ne pas exiger de symboles et de nombres. Cette constatation peut également être déclenchée par une tentative de mise à jour ou de suppression de la politique de mot de passe de votre AWS compte. La politique de mot de passe du AWS compte définit les règles qui régissent les types de mots de passe qui peuvent être définis pour vos utilisateurs IAM. Une stratégie de mots de passe affaiblie permet de créer des mots de passe faciles à mémoriser et potentiellement plus faciles à deviner, ce qui crée un risque de sécurité.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Plusieurs connexions réussies à la console ont été observées dans le monde entier.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que plusieurs connexions réussies à la console de la part du même utilisateur IAM ont été observées simultanément dans divers emplacements géographiques. Ces modèles de localisation d'accès anormaux et risqués indiquent un accès non autorisé potentiel à vos AWS ressources.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Les informations d'identification créées exclusivement pour une instance EC2 via un rôle de lancement d'instance sont utilisées à partir d'un autre compte au sein de AWS.

Gravité par défaut : élevée*

 Note

La gravité par défaut de ce résultat est élevée. Toutefois, si l'API a été invoquée par un compte affilié à votre AWS environnement, le niveau de gravité est moyen.

- Source de données : événements CloudTrail de gestion ou événements de CloudTrail données pour S3

Ce résultat vous indique lorsque les informations d'identification de votre instance Amazon EC2 sont utilisées pour appeler des API à partir d'une adresse IP ou d'un point de terminaison Amazon VPC, qui appartient à un AWS compte différent de celui dans lequel s'exécute l'instance Amazon EC2 associée. La détection des points de terminaison d'un VPC est uniquement disponible pour les services qui prennent en charge les événements d'activité réseau pour les points de terminaison d'un VPC. Pour en savoir plus sur les services qui prennent en charge les événements liés à l'activité du réseau pour les points de terminaison d'un VPC, consultez la section [Journalisation des événements liés à l'activité du réseau](#) dans le Guide de l'utilisateur AWS CloudTrail .

AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exemple, AWS applications, Amazon EC2 ou). AWS Lambda En revanche, les utilisateurs autorisés peuvent exporter les informations d'identification de leurs instances Amazon EC2 pour effectuer des appels d'API légitimes. Si le `remoteAccountDetails.Affiliated` champ est `True` l'API a été invoquée à partir d'un compte associé au même compte administrateur. Pour exclure une attaque potentielle et vérifier la légitimité de l'activité, contactez le Compte AWS propriétaire ou le principal IAM à qui ces informations d'identification sont attribuées.

 Note

S'il GuardDuty observe une activité continue depuis un compte distant, son modèle d'apprentissage automatique (ML) l'identifiera comme un comportement attendu. Par conséquent, GuardDuty cessera de générer ce résultat pour l'activité de ce compte distant. GuardDuty continuera à générer des informations sur les nouveaux comportements d'autres comptes distants et réévaluera les comptes distants appris à mesure que le comportement évolue au fil du temps.

Recommandations de correction :

Ce résultat est généré lorsque des demandes d' AWS API sont effectuées à l'intérieur AWS via une instance Amazon EC2 extérieure à la vôtre Compte AWS, en utilisant les informations d'identification de session de votre instance Amazon EC2. Il peut être habituel, par exemple pour l'architecture Transit Gateway dans une configuration en forme de [hub and spoke](#), d'acheminer le trafic via un seul VPC de sortie de hub AWS avec des points de terminaison de service. Si ce comportement est attendu, il vous GuardDuty recommande d'utiliser [Règles de suppression](#) et de créer une règle avec deux critères de filtre. Le premier critère est le type de résultat, qui, dans ce cas, est UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Le deuxième critère de filtre est l'ID de compte distant contenant les détails du compte distant.

En réponse à ce résultat, vous pouvez utiliser le flux de travail suivant pour déterminer un plan d'action :

1. Identifiez le compte distant concerné depuis le champ `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Déterminez si ce compte est affilié à votre GuardDuty environnement depuis le `service.action.awsApiCallAction.remoteAccountDetails.affiliated` terrain.
3. Si le compte est affilié, contactez son propriétaire distant et le propriétaire des informations d'identification de l'instance Amazon EC2 pour enquêter.

Si le compte n'est pas affilié, la première étape consiste à déterminer s'il est associé à votre organisation mais ne fait pas partie de votre environnement GuardDuty multicompte configuré, ou s'il n' GuardDuty a pas encore été activé dans ce compte. Il faut ensuite contacter le propriétaire des informations d'identification de l'instance Amazon EC2 pour déterminer s'il existe un cas d'utilisation dans lequel un compte distant peut utiliser ces informations d'identification.

4. Si le propriétaire des informations d'identification ne reconnaît pas le compte distant, il est possible que les informations d'identification aient été compromises par un acteur malveillant opérant au sein d' AWS. Vous devez suivre les étapes recommandées dans [Remédier à une instance Amazon EC2 potentiellement compromise](#), pour sécuriser votre environnement.

En outre, vous pouvez [envoyer un rapport d'abus](#) à l'équipe de AWS confiance et de sécurité afin de lancer une enquête sur le compte distant. Lorsque vous soumettez votre rapport à AWS Trust and Safety, incluez tous les détails JSON du résultat.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Des informations d'identification qui ont été créées exclusivement pour une instance EC2 via un rôle de lancement d'instance sont utilisées depuis une adresse IP externe.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion ou événements de CloudTrail données pour S3

Ce résultat vous indique qu'un hôte extérieur AWS a tenté d'exécuter des opérations d' AWS API à l'aide AWS d'informations d'identification temporaires créées sur une instance EC2 de votre AWS environnement. L'instance EC2 répertoriée est peut-être compromise et les informations d'identification temporaires de cette instance ont peut-être été exfiltrées vers un hôte distant situé à l'extérieur de. AWS AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exemple, AWS applications, EC2 ou Lambda). En revanche, les utilisateurs autorisés peuvent exporter les informations d'identification de leurs instances EC2 pour effectuer des appels d'API légitimes. Pour exclure une attaque potentielle et vérifier la légitimité de l'activité, vérifiez si l'utilisation des informations d'identification de l'instance provenant de l'adresse IP distante dans le résultat est prévue.

Note

S'il GuardDuty observe une activité continue d'un hôte distant, son modèle d'apprentissage automatique (ML) l'identifiera comme un comportement attendu. Par conséquent, GuardDuty cessera de générer ce résultat pour l'activité de cet hôte distant. GuardDuty continuera à générer des informations sur les nouveaux comportements d'autres hôtes distants et réévaluera les hôtes distants appris à mesure que le comportement évolue au fil du temps.

Recommandations de correction :

Ce résultat est généré lorsque la mise en réseau est configurée pour acheminer le trafic Internet de telle sorte qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet VPC (IGW). Les configurations courantes, telles que [AWS Outposts](#) ou les connexions VPN VPC, peuvent entraîner l'acheminement du trafic de cette façon. Si ce comportement est attendu, nous vous recommandons

d'utiliser des règles de suppression et de créer une règle composée de deux critères de filtrage. Le premier critère est le type de résultat, qui devrait être `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Le deuxième critère de filtre est l'adresse IPv4 de l'appelant d'API avec l'adresse IP ou la plage d'adresses CIDR de votre passerelle Internet sur site. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression dans GuardDuty](#).

 Note

S'il GuardDuty observe une activité continue provenant d'une source externe, son modèle d'apprentissage automatique identifiera ce comportement comme attendu et cessera de générer ce résultat pour l'activité provenant de cette source. GuardDuty continuera à générer des résultats concernant de nouveaux comportements à partir d'autres sources et réévaluera les sources apprises à mesure que les comportements évoluent au fil du temps.

Si cette activité est inattendue, vos informations d'identification peuvent être compromises, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Une API a été invoquée depuis une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API (par exemple, une tentative de lancer une instance EC2, de créer un utilisateur IAM ou de modifier vos privilèges AWS) a été invoquée depuis une adresse IP malveillante connue. Cela peut indiquer un accès non autorisé aux AWS ressources de votre environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Une API a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une opération d'API (par exemple, une tentative de lancement d'une instance EC2, de création d'un nouvel utilisateur IAM ou de modification de AWS privilèges) a été invoquée à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. Dans GuardDuty, une liste de menaces est composée d'adresses IP malveillantes connues. Cela peut indiquer un accès non autorisé aux AWS ressources de votre environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS

Informations d'identification créées exclusivement pour un AWS Tâche Amazon ECS ou AWS Les fonctions Lambda sont utilisées depuis un autre compte dans AWS

Gravité par défaut : élevée*

Note

La gravité par défaut de ce résultat est élevée. Toutefois, si l'API a été invoquée par un compte affilié à votre AWS environnement, le niveau de gravité est moyen.

- Source de données : événements CloudTrail de gestion ou événements de CloudTrail données pour S3

Ce résultat vous indique lorsque vos informations d'identification de tâche AWS Amazon ECS ou vos informations d'identification de fonction AWS Lambda sont utilisées pour appeler des API à

partir d'une adresse IP ou d'un point de terminaison Amazon VPC, qui appartient à un AWS compte différent de celui sur lequel s'exécute la ressource associée. La détection des points de terminaison d'un VPC est uniquement disponible pour les services qui prennent en charge les événements d'activité réseau pour les points de terminaison d'un VPC. Pour en savoir plus sur les services qui prennent en charge les événements liés à l'activité du réseau pour les points de terminaison d'un VPC, consultez la section [Journalisation des événements liés à l'activité du réseau](#) dans le Guide de l'utilisateur AWS CloudTrail .

AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exemple, les AWS applications, Amazon EC2 ou Amazon Elastic Container Service). Toutefois, les utilisateurs autorisés peuvent exporter des informations d'identification depuis leurs ressources pour effectuer des appels d'API légitimes. Si le `remoteAccountDetails.affiliated` champ est défini comme `True` tel, cela signifie que l'API a été invoquée à partir d'un compte associé au même compte administrateur. Pour exclure une attaque potentielle et vérifier la légitimité de l'activité, contactez le Compte AWS propriétaire ou le principal IAM à qui ces informations d'identification sont attribuées.

Note

S'il GuardDuty observe une activité continue depuis un compte distant, son modèle d'apprentissage automatique (ML) l'identifiera comme un comportement attendu. Par conséquent, GuardDuty cessera de générer ce résultat pour l'activité de ce compte distant. GuardDuty continuera à générer des informations sur les nouveaux comportements d'autres comptes distants et réévaluera les comptes distants appris à mesure que le comportement évolue au fil du temps.

Note

Pour les tâches Amazon ECS, les informations d'identification sont associées au rôle de tâche et la détection s'applique quelle que soit la configuration du VPC.

Recommandations de correction :

Ce résultat est généré lorsque des demandes d' AWS API sont effectuées AWS via une ressource extérieure à la votre Compte AWS, en utilisant vos informations d'identification de tâche AWS Amazon ECS ou vos informations d'identification de fonction AWS Lambda. Il

peut être habituel, par exemple pour l'architecture Transit Gateway dans une configuration en forme de [hub and spoke](#), d'acheminer le trafic via un seul VPC de sortie de hub AWS avec des points de terminaison de service. Si ce comportement est attendu, nous vous recommandons de l'utiliser [Règles de suppression](#) avec le type de recherche par critère de filtre, qui devrait être `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS`.

En réponse à ce résultat, vous pouvez utiliser le flux de travail suivant pour déterminer un plan d'action :

1. Identifiez le compte distant concerné depuis le champ `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Déterminez si ce compte est affilié à votre GuardDuty environnement depuis le `service.action.awsApiCallAction.remoteAccountDetails.affiliated` terrain.
3. Si le compte est affilié, contactez le propriétaire du compte distant et le propriétaire des informations d'identification de la ressource pour enquêter.

Si le compte n'est pas affilié, la première étape consiste à déterminer s'il est associé à votre organisation mais ne fait pas partie de votre environnement GuardDuty multicompte configuré, ou s'il n' GuardDuty a pas encore été activé dans ce compte. Contactez ensuite le propriétaire des informations d'identification de la ressource pour déterminer s'il existe un cas d'utilisation permettant à un compte distant d'utiliser ces informations d'identification.

4. Si le propriétaire des informations d'identification ne reconnaît pas le compte distant, il est possible que les informations d'identification aient été compromises par un acteur malveillant opérant au sein d' AWS. Vous devez suivre les étapes recommandées dans [Remédier à un cluster ECS potentiellement compromis](#), pour sécuriser votre environnement.

En outre, vous pouvez [envoyer un rapport d'abus](#) à l'équipe de AWS confiance et de sécurité afin de lancer une enquête sur le compte distant. Lorsque vous soumettez votre rapport à AWS Trust and Safety, incluez tous les détails JSON du résultat.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS

Informations d'identification créées exclusivement pour un AWS les ressources (une fonction Lambda ou une tâche Amazon ECS) sont utilisées à partir d'une adresse IP extérieure à AWS.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion ou événements de CloudTrail données pour S3

Ce résultat vous indique qu'un hôte externe AWS a tenté d'exécuter des opérations d' AWS API à l'aide d'informations d'identification temporaires créées sur une AWS ressource (une fonction Lambda ou une tâche Amazon ECS) de votre AWS environnement. La ressource répertoriée est peut-être compromise et les informations d'identification temporaires de cette ressource ont peut-être été exfiltrées vers un hôte distant extérieur à AWS.

AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exemple, AWS des applications telles qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service ou). AWS Lambda Toutefois, les utilisateurs autorisés peuvent exporter des informations d'identification depuis leurs ressources pour effectuer des appels d'API légitimes. Pour exclure une attaque potentielle et vérifier la légitimité de l'activité, validez si l'utilisation des informations d'identification de ressource provenant de l'adresse IP distante est prévue pour la découverte.

 Note

S'il GuardDuty observe une activité continue d'un hôte distant, son modèle d'apprentissage automatique (ML) l'identifiera comme un comportement attendu. Par conséquent, GuardDuty cessera de générer ce résultat pour l'activité de cet hôte distant. GuardDuty continuera à générer des informations sur les nouveaux comportements d'autres hôtes distants et réévaluera les hôtes distants appris à mesure que le comportement évolue au fil du temps.

Recommandations de correction :

Ce résultat est généré lorsque la mise en réseau est configurée pour router le trafic Internet afin qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet de VPC (IGW). Les configurations courantes, utilisant par exemple [AWS Outposts](#) ou des connexions VPN de VPC, peuvent entraîner le routage du trafic de cette façon. Si ce comportement est attendu, il est GuardDuty recommandé de l'utiliser [Règles de suppression](#) pour créer une règle avec un critère à deux filtres. Le premier critère est le type de résultat, qui devrait être `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS`. Le deuxième critère de filtre est l'adresse IPv4 de l'appelant d'API avec l'adresse IP ou la plage d'adresses CIDR de votre passerelle Internet sur site.

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations sur les étapes à suivre pour remédier à ce type de recherche [Remédier aux failles potentiellement compromises AWS informations d'identification](#), consultez ou [Remédier à un cluster ECS potentiellement compromis](#).

UnauthorizedAccess:IAMUser/TorIPCaller

Une API a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API (par exemple, une tentative de lancer une instance EC2, de créer un utilisateur IAM ou de modifier vos privilèges AWS) a été invoquée depuis une adresse IP de nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à vos ressources AWS dans le but de masquer la véritable identité du pirate.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

GuardDuty types de recherche de séquences d'attaque

GuardDuty détecte une séquence d'attaque lorsqu'une séquence spécifique de plusieurs actions correspond à une activité potentiellement suspecte. Une séquence d'attaque inclut des signaux tels que les activités et les GuardDuty résultats de l'API. Lorsqu'il GuardDuty observe un groupe de signaux dans une séquence spécifique qui indique une menace de sécurité en cours, en cours ou récente, GuardDuty génère une recherche de séquence d'attaque. GuardDuty considère les activités d'API individuelles comme [weak signals](#) étant le fait qu'elles ne se présentent pas comme une menace potentielle.

Les détections de séquences d'attaques se concentrent sur la compromission potentielle des données Amazon S3 (qui peut faire partie d'une attaque de rançongiciel plus large), les AWS

informations d'identification compromises, les clusters Amazon EKS compromis, les clusters Amazon ECS compromis et les groupes d'instances Amazon EC2 compromis. Les sections suivantes fournissent des détails sur chacune des séquences d'attaque.

Rubriques

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:ECS/CompromisedCluster](#)
- [AttackSequence:EC2/CompromisedInstanceGroup](#)
- [AttackSequence:IAM/CompromisedCredentials](#)
- [AttackSequence:S3/CompromisedData](#)

AttackSequence:EKS/CompromisedCluster

Séquence d'actions suspectes effectuées par un cluster Amazon EKS potentiellement compromis.

- Gravité par défaut : Critique
- Sources de données :
 - [Événements du journal d'audit EKS](#)
 - [Surveillance de l'exécution pour Amazon EKS](#)
 - [Détection des programmes malveillants Amazon EKS pour Amazon EC2](#)
 - [AWS CloudTrail événements de données pour S3](#)
 - [AWS CloudTrail événements de gestion](#)
 - [Journaux de flux VPC](#)
 - [Journaux de requêtes DNS de Route53 Resolver](#)

Cette découverte vous indique qu'une séquence d'actions suspectes a GuardDuty été détectée indiquant la présence d'un cluster Amazon EKS potentiellement compromis dans votre environnement. De multiples comportements d'attaque suspects et anormaux, tels que des processus malveillants ou des connexions à des terminaux malveillants, ont été observés dans le même cluster Amazon EKS.

GuardDuty utilise ses algorithmes de corrélation propriétaires pour observer et identifier la séquence d'actions effectuées à l'aide de l'identifiant IAM. GuardDuty évalue les résultats des plans de

protection et d'autres sources de signaux afin d'identifier les modèles d'attaque courants et émergents. GuardDuty utilise plusieurs facteurs pour identifier les menaces, tels que la réputation IP, les séquences d'API, la configuration utilisateur et les ressources potentiellement touchées.

Actions correctives : si ce comportement est inattendu dans votre environnement, il est possible que votre cluster Amazon EKS soit compromis. Pour obtenir des conseils de remédiation complets, reportez-vous aux sections [Corriger les résultats de la protection EKS](#) et [Correction des résultats de la surveillance d'exécution](#)

En outre, étant donné que les AWS informations d'identification peuvent avoir été compromises via le cluster EKS, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#). Pour connaître les étapes à suivre pour remédier à d'autres ressources susceptibles d'avoir été potentiellement affectées, consultez [Corriger les problèmes de GuardDuty sécurité détectés](#).

AttackSequence:ECS/CompromisedCluster

Séquence d'actions suspectes effectuées par un cluster Amazon ECS potentiellement compromis.

- Gravité par défaut : Critique
- Sources de données :
 - [Surveillance de l'exécution pour Amazon ECS Fargate](#)
 - [Surveillance de l'exécution des instances EC2 dans Amazon ECS](#)
 - [GuardDuty Protection contre les programmes malveillants pour Amazon EC2](#)

Cette découverte vous indique qu'une séquence de signaux suspects a GuardDuty été détectée indiquant la présence d'un cluster Amazon ECS potentiellement compromis dans votre environnement. Ces signaux peuvent inclure des processus malveillants, des communications avec des terminaux malveillants ou des comportements d'extraction de cryptomonnaies.

GuardDuty utilise des algorithmes de corrélation propriétaires et de multiples facteurs de détection pour identifier les séquences d'actions suspectes au sein des clusters Amazon ECS. Grâce à l'analyse des plans de protection et des différentes sources de signaux, GuardDuty identifie les modèles d'attaque courants et émergents, fournissant une détection fiable des compromissions potentielles.

Actions correctives : si ce comportement est inattendu dans votre environnement, votre cluster Amazon ECS est peut-être compromis. Pour les recommandations relatives au confinement des menaces, consultez [Remédier à un cluster ECS potentiellement compromis](#). Notez que le compromis peut s'étendre à une ou plusieurs tâches ECS ou charges de travail de conteneurs, qui auraient pu être utilisées pour créer ou modifier AWS des ressources. Pour obtenir des conseils de remédiation complets couvrant les ressources potentiellement touchées, consultez [Corriger les problèmes de GuardDuty sécurité détectés](#).

AttackSequence:EC2/CompromisedInstanceGroup

Séquence d'actions suspectes indiquant des instances Amazon EC2 potentiellement compromises.

- Gravité par défaut : Critique
- Sources de données :
 - [Surveillance de l'exécution pour Amazon EC2](#)
 - [Détection des programmes malveillants pour Amazon EC2](#)
 - [Journaux de flux VPC](#)
 - [Journaux de requêtes DNS de Route53 Resolver](#)

Cette découverte indique la GuardDuty détection d'une séquence d'actions suspectes suggérant une compromission potentielle au sein d'un groupe d'instances Amazon EC2 de votre environnement. Les groupes d'instances représentent généralement des applications gérées via l'infrastructure en tant que code, partageant des configurations similaires telles que le Auto-scaling groupe, le rôle du profil d'instance IAM, la AWS CloudFormation pile, le modèle de lancement Amazon EC2, l'AMI ou l'ID VPC. GuardDuty a observé plusieurs comportements suspects dans une ou plusieurs instances, notamment :

- Procédés malveillants
- Fichiers malveillants
- Connexions réseau suspectes
- Activités de minage de cryptomonnaies
- Utilisation suspecte des informations d'identification de l'instance Amazon EC2

Méthode de détection : GuardDuty utilise des algorithmes de corrélation propriétaires pour identifier les séquences d'actions suspectes au sein des instances Amazon EC2. En évaluant les résultats des plans de protection et des différentes sources de signaux, GuardDuty identifie les modèles d'attaque à l'aide de plusieurs facteurs tels que la réputation de l'adresse IP et du domaine et les processus d'exécution suspects.

Actions correctives : si ce comportement est inattendu dans votre environnement, il est possible que vos instances Amazon EC2 soient compromises. Le compromis pourrait impliquer :

- Procédés multiples
- Informations d'identification d'instance qui peuvent avoir été utilisées pour modifier des instances Amazon EC2 ou d'autres ressources AWS

Pour les recommandations relatives au confinement des menaces, consultez [Remédier à une instance Amazon EC2 potentiellement compromise](#). Notez que la compromission peut s'étendre à une ou plusieurs instances Amazon EC2 et impliquer des processus compromis ou des informations d'identification d'instance qui auraient pu être utilisées pour créer ou modifier des instances Amazon EC2 ou d'autres AWS ressources. Pour obtenir des conseils de remédiation complets couvrant les ressources potentiellement touchées, consultez [Corriger les problèmes de GuardDuty sécurité détectés](#).

AttackSequence:IAM/CompromisedCredentials

Une séquence de requêtes d'API qui ont été invoquées à l'aide d'une méthode potentiellement compromise AWS informations d'identification.

- Sévérité par défaut : Critique
- Source de données : [AWS CloudTrail événements de gestion](#)

Cette découverte vous indique qu'une séquence d'actions suspectes a GuardDuty été détectée à l'aide d' AWS informations d'identification qui ont un impact sur une ou plusieurs ressources de votre environnement. De multiples comportements d'attaque suspects et anormaux ont été observés par les mêmes informations d'identification, ce qui a renforcé la certitude que les informations d'identification étaient utilisées à mauvais escient.

GuardDuty utilise ses algorithmes de corrélation propriétaires pour observer et identifier la séquence d'actions effectuées à l'aide de l'identifiant IAM. GuardDuty évalue les résultats des plans de

protection et d'autres sources de signaux afin d'identifier les modèles d'attaque courants et émergents. GuardDuty utilise plusieurs facteurs pour identifier les menaces, tels que la réputation IP, les séquences d'API, la configuration utilisateur et les ressources potentiellement touchées.

Lorsque vous l'activez [Protection de l'IA](#), vous GuardDuty pouvez également inclure [Types de détection de protection contre l'IA](#) parmi les signaux qu'il met en corrélation pour cette séquence d'attaque. Ces résultats sont associés à une identité IAM. Par conséquent, ils GuardDuty peuvent les faire apparaître comme des signaux dans cette séquence d'attaque et les mettre en corrélation avec d'autres actions suspectes entreprises avec les mêmes informations d'identification potentiellement compromises. Par exemple, GuardDuty peut corréler d'autres signaux avec une invocation anormale du modèle Amazon Bedrock ou Amazon SageMaker AI faite avec ces informations d'identification, et l'inclure dans cette séquence d'attaque. À eux seuls, les résultats de AI Protection ne génèrent pas de séquence d'attaque. Pour de plus amples informations, veuillez consulter [Protection de l'IA](#).

Actions correctives : si ce comportement est inattendu dans votre environnement, il se peut que vos AWS informations d'identification aient été compromises. Pour connaître les étapes à suivre pour y remédier, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#). Les informations d'identification compromises ont peut-être été utilisées pour créer ou modifier des ressources supplémentaires, telles que des compartiments Amazon S3, des AWS Lambda fonctions ou des instances Amazon EC2, dans votre environnement. Pour connaître les étapes à suivre pour remédier à d'autres ressources susceptibles d'avoir été potentiellement affectées, consultez [Corriger les problèmes de GuardDuty sécurité détectés](#).

AttackSequence:S3/CompromisedData

Une séquence de demandes d'API a été invoquée dans une tentative potentielle d'exfiltration ou de destruction de données dans Amazon S3.

- Sévérité par défaut : Critique
- Sources de données : [AWS CloudTrail événements de données pour S3](#) et [AWS CloudTrail événements de gestion](#)

Cette découverte vous indique qu'une séquence d'actions suspectes a GuardDuty été détectée, indiquant une compromission des données dans un ou plusieurs compartiments Amazon Simple Storage Service (Amazon S3), en utilisant des AWS informations d'identification potentiellement compromises. De multiples comportements d'attaque suspects et anormaux (requêtes d'API) ont été observés, ce qui a permis de garantir une utilisation abusive des informations d'identification.

GuardDuty utilise ses algorithmes de corrélation pour observer et identifier la séquence d'actions effectuées à l'aide de l'identifiant IAM. GuardDuty évalue ensuite les résultats des plans de protection et d'autres sources de signaux afin d'identifier les modèles d'attaque courants et émergents. GuardDuty utilise plusieurs facteurs pour identifier les menaces, tels que la réputation IP, les séquences d'API, la configuration utilisateur et les ressources potentiellement touchées.

Actions correctives : si cette activité est inattendue dans votre environnement, il est possible que vos AWS informations d'identification ou vos données Amazon S3 aient été exfiltrées ou détruites. Pour connaître les étapes à suivre pour y remédier, reportez-vous aux sections [Remédier aux failles potentiellement compromises AWS informations d'identification](#) et [Remédier à un compartiment S3 potentiellement compromis](#)

Règles de détection personnalisées : types de recherche

Cette page répertorie les types de recherche GuardDuty générés à partir de règles de détection personnalisées, regroupés par source de données. Chaque type de recherche agrège un ou plusieurs signaux en un seul résultat. Pour plus d'informations sur l'activation des règles de détection personnalisées, consultez [Règles de détection personnalisées dans GuardDuty](#).

Note

Les règles individuelles ne sont disponibles Régions AWS que si elles prennent en charge le AWS service ou la fonctionnalité qu'elles ciblent. Par exemple, les règles qui ciblent AWS les Organizations ou Amazon Simple Email Service ne sont disponibles que dans les régions où ces services sont disponibles. De même, les règles qui ciblent les URL des fonctions Lambda ou les instances de SageMaker blocs-notes AI ne sont disponibles que dans les régions où ces fonctionnalités sont prises en charge.

Rubriques

- [Règles de détection personnalisées pour AWS CloudTrail événements de gestion](#)
- [Règles de détection personnalisées pour la surveillance du temps d'exécution](#)

Règles de détection personnalisées pour AWS CloudTrail événements de gestion

Les types de résultats suivants sont générés à partir AWS CloudTrail des signaux d'événements de gestion, organisés par MITRE ATT&CK® tactic.

Accès via les informations d'identification

Ces règles tentent de détecter les opérations qui récupèrent ou réinitialisent les informations d'identification, telles que la récupération du mot de passe d'une instance Amazon EC2 ou la réinitialisation d'un mot de passe administrateur Amazon RDS.

Type de résultat	Nom de la règle	Sévérité
CredentialAccess:EC2/UnsecuredCredentials	EC2PasswordDataRetrieved	MOYEN
CredentialAccess:RDS/ModifyAuthenticationProcess	RDSMasterPasswordReset	ÉLEVÉ

Déficiences des défenses

Ces règles tentent de détecter les modifications qui désactivent ou affaiblissent les contrôles de sécurité, telles que la suppression des journaux de flux VPC, la désactivation d'une politique d'entreprise ou la suppression d'un compte d'une organisation.

Type de résultat	Nom de la règle	Sévérité
DefenseImpairment:EC2/DisableOrModifyTools	EC2TerminationProtectionEnabled	BAS
	VPCFlowLogsDeleted	ÉLEVÉ
DefenseImpairment:Organizations/ModifyCloudResourceHierarchy	OrganizationLeaveAttempt	ÉLEVÉ
DefenseImpairment:Organizations/DisableOrModifyTools	OrganizationPolicyDisabled	ÉLEVÉ

Type de résultat	Nom de la règle	Sévérité
DefenseImpairment:RDS/ModifyAuthenticationProcess	RDSIAMAuthDisabled	MOYEN
DefenseImpairment:Route53Resolver/DisableOrModifyTools	DNSQueryLogsDeleted	MOYEN
DefenseImpairment:S3/DisableOrModifyTools	S3CustomerProvidedKeysEnabled	ÉLEVÉ

Exécution

Ces règles tentent de détecter les modifications qui exécutent du code sur une ressource, telles que la modification de la configuration du cycle de vie d'un bloc-notes SageMaker AI.

Type de résultat	Nom de la règle	Sévérité
Execution:SageMaker/CommandAndScriptingInterpreter	SageMakerLifecycleConfigModified	MOYEN

Exfiltration

Ces règles visent à détecter les modifications qui partagent des ressources en dehors de votre compte, par exemple en rendant une AMI, un instantané Amazon EBS ou un instantané Amazon RDS accessibles à d'autres comptes.

Type de résultat	Nom de la règle	Sévérité
Exfiltration:EC2/TransferDataToCloudAccount	AMIExternalAccess	ÉLEVÉ
	EBSSnapshotExternalAccess	ÉLEVÉ
Exfiltration:RDS/TransferDataToCloudAccount	RDSSnapshotPubliclyShared	ÉLEVÉ
Exfiltration:S3/TransferDataToCloudAccount	S3BucketPolicyExternalAccess	ÉLEVÉ

Impact

Ces règles tentent de détecter les modifications susceptibles de perturber ou de détruire les données et les ressources, par exemple en configurant les objets Amazon S3 pour qu'ils expirent rapidement ou en activant l'envoi par Amazon SES.

Type de résultat	Nom de la règle	Sévérité
Impact:S3/DataDestruction	S3LifecycleRapidExpiration	MOYEN
Impact:SES/ResourceHijacking	SESAccountSendingEnabled	BAS
	SESProductionAccessEnabled	MOYEN

Accès initial

Ces règles tentent de détecter les activités qui ouvrent l'accès à votre environnement, comme une connexion à la console sans MFA ou le fait de rendre une base de données Amazon RDS accessible au public.

Type de résultat	Nom de la règle	Sévérité
InitialAccess:IAM/ValidAccounts	ConsoleLoginWithoutMFA	MOYEN
InitialAccess:RDS/ExploitPublicFacingApplication	RDSPubliclyAccessible	ÉLEVÉ

Mouvement latéral

Ces règles tentent de détecter les activités qui accordent l'accès entre les ressources, comme l'envoi d'une clé SSH vers une instance Amazon EC2.

Type de résultat	Nom de la règle	Sévérité
LateralMovement:EC2/RemoteServices	EC2InstanceSSHKeyPushed	MOYEN

Persistence

Ces règles tentent de détecter les modifications qui créent ou étendent l'accès, telles que la création de clés d'accès IAM, la modification d'une politique de confiance des rôles ou le fait de rendre une fonction Lambda accessible au public.

Type de résultat	Nom de la règle	Sévérité
Persistence:EC2/BootOrLogonInitializationScripts	EC2UserDataModified	ÉLEVÉ
Persistence:EC2/ExternalRemoteServices	EC2SecurityGroupPublicSSH	MOYEN
Persistence:IAM/AccountManipulation	IAMAccessKeyCreated	BAS
	IAMRoleTrustPolicyModified	MOYEN
	IAMUserLoginProfileCreated	ÉLEVÉ
	IAMUserLoginProfileUpdated	MOYEN
Persistence:Lambda/AccountManipulation	LambdaFunctionPublicAccess	ÉLEVÉ
Persistence:Lambda/ModifyAuthenticationProcess	LambdaFunctionUrlPublicAccess	ÉLEVÉ
Persistence:RolesAnywhere/AccountManipulation	RolesAnywhereTrustAnchorCreated	MOYEN

Escalade de privilèges

Ces règles tentent de détecter les modifications qui accordent des autorisations plus étendues, telles que l'association d'une politique d'administrateur à un utilisateur ou à un rôle IAM.

Type de résultat	Nom de la règle	Sévérité
PrivilegeEscalation:IAM/AccountManipulation	AdminPolicyAttachedToRole	ÉLEVÉ
	AdminPolicyAttachedToUser	ÉLEVÉ

Type de résultat	Nom de la règle	Sévérité
	BedrockServiceCredentialCreated	MOYEN
	SESFullAccessPolicyAttachedToRole	MOYEN
	SESFullAccessPolicyAttachedToUser	MOYEN

Développement des ressources

Ces règles tentent de détecter la configuration de ressources susceptibles de prendre en charge des activités ultérieures, telles que la vérification de l'identité d'un domaine Amazon SES.

Type de résultat	Nom de la règle	Sévérité
ResourceDevelopment:SES/CompromiseAccounts	SESDomainIdentityVerified	MOYEN

Règles de détection personnalisées pour la surveillance du temps d'exécution

GuardDuty génère les règles de détection personnalisées suivantes pour trouver les types à partir des signaux de surveillance du temps d'exécution, organisés par tactique MITRE ATT&CK®. Ces règles nécessitent la surveillance du temps d'exécution et l'agent GuardDuty de sécurité sur la ressource surveillée. Pour plus d'informations, consultez [Sources de données et signaux](#).

Commande et contrôle

Ces règles tentent de détecter les processus qui acheminent le trafic réseau, tels que les outils de tunneling DNS ou le tunneling de protocole.

Type de résultat	Nom de la règle	Sévérité
CommandAndControl:Runtime/SuspiciousCommand	DnsTunnelingToolExecuted	ÉLEVÉ

Type de résultat	Nom de la règle	Sévérité
CommandAndControl:Runtime/SuspiciousCommand	SuspiciousProtocolTunneling	MOYEN

Accès via les informations d'identification

Ces règles tentent de détecter les processus qui lisent des données sensibles, telles que la mémoire des processus via le système de /proc fichiers.

Type de résultat	Nom de la règle	Sévérité
CredentialAccess:Runtime/SensitiveFileRead	DumpProcessMemoryFromProc	ÉLEVÉ

Déficiences des défenses

Ces règles tentent de détecter les processus qui affaiblissent les défenses de l'hôte, tels que la désactivation de la journalisation des audits, la modification des règles de pare-feu ou l'arrêt des services.

Type de résultat	Nom de la règle	Sévérité
DefenseEvasion:Runtime/SensitiveFileModified	FirewallConfigModified	MOYEN
DefenseEvasion:Runtime/SensitiveFileModified	LogManipulation	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	AuditDisabled	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	FirewallDisablement	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	KernelHardeningDisabled	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	KillCommandUsage	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	ServiceStoppedOrDisabled	MOYEN

Découverte

Ces règles tentent de détecter les processus qui collectent des informations sur une ressource, tels que la lecture de fichiers de mots de passe, la recherche d'informations d'identification ou de clés, ou la détection de la virtualisation.

Type de résultat	Nom de la règle	Sévérité
Discovery:Runtime/SensitiveFileRead	PasswordShadowFileDiscovery	MOYEN
Discovery:Runtime/SuspiciousCommand	FindCommandReconCloudCredent tials	MOYEN
Discovery:Runtime/SuspiciousCommand	FindCommandReconKeyMaterial	MOYEN
Discovery:Runtime/SuspiciousCommand	PromiscuousModeEnabled	MOYEN
Discovery:Runtime/SuspiciousCommand	SSHWithHostKeyCheckingDisab led	MOYEN
Discovery:Runtime/SuspiciousCommand	SqliteDatabaseDump	BAS
Discovery:Runtime/SuspiciousCommand	VirtualizationDetection	BAS

Exécution

Ces règles tentent de détecter les processus qui exécutent des commandes ou du code potentiellement malveillants, tels que le téléchargement et l'exécution d'un script ou l'ouverture d'un shell interactif dans un conteneur.

Type de résultat	Nom de la règle	Sévérité
Execution:Runtime/SuspiciousCommand	ChmodInTmpDirectory	MOYEN
Execution:Runtime/SuspiciousCommand	CurlWgetScriptDownload	MOYEN
Execution:Runtime/SuspiciousCommand	DataEncryptionUsingCommandL ineUtilities	MOYEN

Type de résultat	Nom de la règle	Sévérité
Execution:Runtime/SuspiciousCommand	InlinePythonExecution	MOYEN
Execution:Runtime/SuspiciousCommand	InteractiveShellInsideAContainer	MOYEN
Execution:Runtime/SuspiciousCommand	RemoteFileCopy	MOYEN
Execution:Runtime/SuspiciousCommand	ShellFromUtilities	MOYEN
Execution:Runtime/SuspiciousTool	NetworkSnifferToolExecuted	MOYEN
Execution:Runtime/SuspiciousTool	RawSocketCreated	MOYEN

Exfiltration

Ces règles tentent de détecter les processus qui déplacent des données hors d'une ressource, tels que le téléchargement de fichiers avec curl, wget ou rclone, ou le fractionnement de données avant le transfert.

Type de résultat	Nom de la règle	Sévérité
Exfiltration:Runtime/SuspiciousCommand	CurlWgetExfiltrateData	MOYEN
Exfiltration:Runtime/SuspiciousCommand	DataSplittingForExfiltration	MOYEN
Exfiltration:Runtime/SuspiciousCommand	S3DataExfiltrationWithRclone	MOYEN

Persistence

Ces règles tentent de détecter les modifications qui permettent de conserver l'accès à une ressource, telles que la modification de comptes utilisateurs, de clés autorisées SSH, de tâches planifiées ou de services système.

Type de résultat	Nom de la règle	Sévérité
Persistence:Runtime/SensitiveFileModified	PAMConfigModification	MOYEN

Type de résultat	Nom de la règle	Sévérité
Persistence:Runtime/SensitiveFileModified	PasswordModification	MOYEN
Persistence:Runtime/SensitiveFileModified	SSHAuthorizedKeysModification	MOYEN
Persistence:Runtime/SensitiveFileModified	ScheduledJobManipulation	MOYEN
Persistence:Runtime/SensitiveFileModified	ShellRCFileManipulated	MOYEN
Persistence:Runtime/SensitiveFileModified	SystemdServiceManipulation	MOYEN
Persistence:Runtime/SuspiciousCommand	AuditdKeylogger	MOYEN
Persistence:Runtime/SuspiciousCommand	InteractiveLocalAccountCreation	MOYEN
Persistence:Runtime/SuspiciousCommand	NobodyUserManipulation	ÉLEVÉ
Persistence:Runtime/SuspiciousCommand	SshFromPublicIPAddress	MOYEN
Persistence:Runtime/SuspiciousCommand	SystemdTransientServiceCreated	MOYEN

Escalade de privilèges

Ces règles tentent de détecter les modifications qui accordent des autorisations de niveau supérieur, telles que la modification de fichiers sudoers, la définition de l'indicateur setuid ou l'évasion d'un conteneur avec nsenter.

Type de résultat	Nom de la règle	Sévérité
DefenseEvasion:Runtime/SuspiciousCommand	FindCommandReconSetuidSetgidFiles	MOYEN
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileLinked	MOYEN
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileManipulation	MOYEN

Type de résultat	Nom de la règle	Sévérité
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileRenamed	MOYEN
PrivilegeEscalation:Runtime/SuspiciousCommand	AddSetUIDCapability	ÉLEVÉ
PrivilegeEscalation:Runtime/SuspiciousCommand	NewUserAddedToRootGroup	ÉLEVÉ
PrivilegeEscalation:Runtime/SuspiciousCommand	NsenterContainerEscape	ÉLEVÉ
PrivilegeEscalation:Runtime/SuspiciousCommand	SetUidFlagSet	MOYEN
PrivilegeEscalation:Runtime/SuspiciousCommand	SudoPrivilegeEnumeration	MOYEN
PrivilegeEscalation:Runtime/SuspiciousCommand	SudoerFileRead	MOYEN

Stealth

Ces règles tentent de détecter les processus qui masquent une activité, tels que le piratage de fonctions de bibliothèque avec LD_PRELOAD ou le codage de données avec Base64.

Type de résultat	Nom de la règle	Sévérité
DefenseEvasion:Runtime/SensitiveFileModified	LDPreloadFunctionHijack	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	Base64EncodeDecode	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	BpftoolProgramLoaded	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	DebugfsRawDiskAccess	MOYEN
DefenseEvasion:Runtime/SuspiciousCommand	SuspiciousExecutionPath	MOYEN

GuardDuty Types de détection de la protection S3

Les résultats suivants sont spécifiques aux ressources Amazon S3 et auront un type de ressource selon S3Bucket que la source de CloudTrail données est constituée d'événements de données pour S3 ou AccessKey d'événements CloudTrail de gestion. La gravité et les détails des résultats diffèrent selon le type de résultat et l'autorisation associée au compartiment.

Les résultats répertoriés ici incluent les sources de données et les modèles utilisés pour générer ce type de résultat. Pour plus d'informations sur les sources de données et les modèles, veuillez consulter [GuardDuty sources de données de base](#).

Important

Les résultats contenant une source de CloudTrail données contenant des événements de données pour S3 ne sont générés que si vous avez activé S3 Protection. Par défaut, après le 31 juillet 2020, S3 Protection est activée lorsqu'un compte est activé GuardDuty pour la première fois ou lorsqu'un compte d'administrateur délégué est activé GuardDuty dans un compte membre existant. Toutefois, lorsqu'un nouveau membre rejoint l'organisation, les préférences d'activation automatique de l'organisation s'appliquent. Pour plus d'informations sur les préférences d'activation automatique, consultez [Configuration des préférences d'activation automatique de l'organisation](#). Pour plus d'informations sur l'activation de la protection S3, consultez [GuardDuty Protection S3](#).

Pour tous les résultats de type S3Bucket, il est recommandé d'examiner les autorisations sur le compartiment en question et les autorisations de tous les utilisateurs impliqués dans le résultat. Si l'activité est inattendue, veuillez consulter les recommandations de correction détaillées dans [Remédier à un compartiment S3 potentiellement compromis](#).

Rubriques

- [Discovery:S3/AnomalousBehavior](#)
- [Discovery:S3/MaliciousIPCaller](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:S3/MaliciousIPCaller](#)

- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/MaliciousIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [PenTest:S3/ParrotLinux](#)
- [PenTest:S3/PentooLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)

Discovery:S3/AnomalousBehavior

Une API couramment utilisée pour découvrir des objets S3 a été invoquée de manière anormale.

Gravité par défaut : faible

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une entité IAM a invoqué une API S3 pour découvrir des compartiments S3 dans votre environnement, comme `ListObjects`. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un attaquant recueille des informations pour déterminer si votre AWS environnement est vulnérable à une attaque de plus grande envergure. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre

compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, consultez [Détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Discovery:S3/MaliciousIPCaller

Une API S3 couramment utilisée pour découvrir des ressources dans un AWS l'environnement a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3 a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à la phase de découverte d'une attaque lorsqu'un adversaire collecte des informations sur votre AWS environnement. Exemples : `GetObjectAcl` et `ListObjects`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Discovery:S3/MaliciousIPCaller.Custom

Une API S3 a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une API S3, comme `GetObjectAcl` ou `ListObjects`, a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un pirate collecte des informations pour déterminer si votre environnement AWS est vulnérable à une attaque de plus grande envergure.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Discovery:S3/TorIPCaller

Une API S3 a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une API S3, comme `GetObjectAcl` ou `ListObjects`, a été invoquée depuis une adresse IP du nœud de sortie Tor. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un attaquant collecte des informations pour déterminer si votre AWS environnement est vulnérable à une attaque de plus grande envergure. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut indiquer un accès non autorisé à vos AWS ressources dans le but de masquer la véritable identité de l'attaquant.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Exfiltration:S3/AnomalousBehavior

Une entité IAM a invoqué une API S3 de manière suspecte.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une entité IAM effectue des appels d'API qui impliquent un compartiment S3 et que cette activité diffère de la référence établie de cette entité. L'appel d'API utilisé dans cette activité est associé à la phase d'exfiltration d'une attaque, au cours de laquelle un pirate tente de collecter des données. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, consultez [Détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Exfiltration:S3/MaliciousIPCaller

Une API S3 couramment utilisée pour collecter des données à partir d'un AWS l'environnement a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3 a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques d'exfiltration dans le cadre desquelles un adversaire tente de collecter des données sur votre réseau. Exemples : `GetObject` et `CopyObject`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Impact:S3/AnomalousBehavior.Delete

Une entité IAM a invoqué une API S3 qui tente de supprimer des données de manière suspecte.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une entité IAM de votre AWS environnement effectue des appels d'API impliquant un compartiment S3 et que ce comportement diffère de la référence établie par cette entité. L'appel d'API utilisé dans cette activité est associé à une attaque visant à supprimer des données. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre

compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, consultez [Détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Nous recommandons un audit du contenu de votre compartiment S3 afin de déterminer si la version précédente de l'objet peut ou doit être restaurée.

Impact:S3/AnomalousBehavior.Permission

Une API couramment utilisée pour définir les autorisations de liste de contrôle d'accès (ACL) a été invoquée de manière anormale.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une entité IAM de votre AWS environnement a mis à jour une politique de compartiment ou une ACL sur les compartiments S3 répertoriés. Cette modification peut exposer publiquement vos compartiments S3 à tous les utilisateurs authentifiés. AWS

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, consultez [Détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Nous recommandons un audit du contenu de votre compartiment S3 pour vous assurer qu'aucun objet n'a été autorisé à être consulté publiquement de manière inattendue.

Impact:S3/AnomalousBehavior.Write

Une entité IAM a invoqué une API S3 qui tente d'écrire des données de manière suspecte.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une entité IAM de votre AWS environnement effectue des appels d'API impliquant un compartiment S3 et que ce comportement diffère de la référence établie par cette entité. L'appel d'API utilisé dans cette activité est associé à une attaque qui tente d'écrire des données. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, consultez [Détails du résultat](#).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Nous recommandons un audit du contenu de votre compartiment S3 pour vous assurer que cet appel d'API n'a pas écrit de données malveillantes ou non autorisées.

Impact:S3/MaliciousIPCaller

Une API S3 couramment utilisée pour modifier des données ou des processus dans un AWS l'environnement a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3 a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données dans votre AWS environnement. Exemples : PutObject et PutObjectAcl.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

PenTest:S3/KaliLinux

Une API S3 a été invoquée par une machine Kali Linux.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une machine exécutant Kali Linux effectue des appels d'API S3 à l'aide d'informations d'identification appartenant à votre AWS compte. Vos informations d'identification pourraient être compromises. Kali Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de la configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

PenTest:S3/ParrotLinux

Une API S3 a été invoquée par une machine Parrot Security Linux.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une machine exécutant Parrot Security Linux effectue des appels d'API S3 à l'aide d'informations d'identification appartenant à votre AWS compte. Vos informations d'identification pourraient être compromises. Parrot Security Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les pirates utilisent également cet outil pour identifier les faiblesses de la configuration EC2 et accéder à votre environnement AWS sans y être autorisés.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

PenTest:S3/PentooLinux

Une API S3 a été invoquée par une machine Pentoo Linux.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une machine exécutant Pentoo Linux effectue des appels d'API S3 à l'aide d'informations d'identification appartenant à votre AWS compte. Vos informations

d'identification pourraient être compromises. Pentoo Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de la configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Policy:S3/AccountBlockPublicAccessDisabled

Une entité IAM a invoqué une API utilisée pour désactiver le blocage de l'accès public S3 sur un compte.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que le blocage de l'accès public Amazon S3 a été désactivé au niveau du compte. Lorsque les paramètres de blocage de l'accès public S3 sont activés, ils sont utilisés pour filtrer les stratégies ou les listes de contrôle d'accès (ACL) sur les compartiments en tant que mesure de sécurité afin d'empêcher l'exposition publique accidentelle des données.

Généralement, le blocage de l'accès public S3 est désactivé dans un compte pour autoriser l'accès public à un compartiment ou aux objets du compartiment. Lorsque le blocage de l'accès public S3 est désactivé pour un compte, l'accès à vos compartiments est contrôlé par les stratégies, les ACL ou les paramètres de blocage de l'accès public au niveau du compartiment appliqués à vos compartiments individuels. Cela ne signifie pas nécessairement que les compartiments sont partagés publiquement, mais que vous devez auditer les autorisations appliquées aux compartiments pour confirmer qu'elles fournissent le niveau d'accès approprié.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Policy:S3/BucketAnonymousAccessGranted

Un principal IAM a accordé l'accès à un compartiment S3 à Internet en modifiant les stratégies de compartiment ou les ACL.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que le compartiment S3 répertorié a été rendu public sur Internet, car une entité IAM a modifié une stratégie de compartiment ou une ACL sur ce compartiment.

Une fois qu'une modification de politique ou d'ACL est détectée, GuardDuty utilise un raisonnement automatique alimenté par [Zelkova](#) pour déterminer si le compartiment est accessible au public.

Note

Si les ACL ou les stratégies de compartiment d'un compartiment sont configurées pour tout refuser ou refuser explicitement, ce résultat peut ne pas refléter l'état actuel du compartiment. Ce résultat ne reflétera aucun paramètre de [blocage de l'accès public S3](#) qui aurait pu être activé pour votre compartiment S3. Dans de tels cas, la valeur effectivePermission du résultat sera marquée comme UNKNOWN.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Policy:S3/BucketBlockPublicAccessDisabled

Une entité IAM a invoqué une API utilisée pour désactiver le blocage de l'accès public S3 sur un compartiment.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que le blocage de l'accès public a été désactivé pour le compartiment S3 répertorié. Lorsque les paramètres de blocage de l'accès public S3 sont activés, ils sont utilisés pour filtrer les stratégies ou les listes de contrôle d'accès (ACL) appliquées aux compartiments en tant que mesure de sécurité afin d'empêcher l'exposition publique accidentelle des données.

Généralement, le blocage de l'accès public S3 est désactivé sur un compartiment pour autoriser l'accès public au compartiment ou aux objets qu'il contient. Lorsque le blocage de l'accès public S3 est désactivé pour un compartiment, les stratégies ou listes ACL appliquées au compartiment en contrôlent l'accès. Cela ne signifie pas que le compartiment est partagé publiquement, mais vous devez auditer les stratégies et les listes ACL appliquées au compartiment pour confirmer que les autorisations appropriées sont appliquées.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Policy:S3/BucketPublicAccessGranted

Un principal IAM a accordé l'accès public à un compartiment S3 à tous AWS utilisateurs en modifiant les politiques de bucket ou les ACL.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion

Cette découverte vous indique que le compartiment S3 répertorié a été exposé publiquement à tous les AWS utilisateurs authentifiés car une entité IAM a modifié une politique de compartiment ou une ACL sur ce compartiment S3.

Une fois qu'une modification de politique ou d'ACL est détectée, GuardDuty utilise un raisonnement automatique alimenté par [Zelkova](#) pour déterminer si le compartiment est accessible au public.

Note

Si les ACL ou les stratégies de compartiment d'un compartiment sont configurées pour tout refuser ou refuser explicitement, ce résultat peut ne pas refléter l'état actuel du compartiment.

Ce résultat ne reflétera aucun paramètre de [blocage de l'accès public S3](#) qui aurait pu être activé pour votre compartiment S3. Dans de tels cas, la valeur effective `Permission` du résultat sera marquée comme UNKNOWN.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Stealth:S3/ServerAccessLoggingDisabled

La journalisation des accès au serveur S3 a été désactivée pour un compartiment.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Cette découverte vous indique que la journalisation des accès au serveur S3 est désactivée pour un compartiment de votre AWS environnement. Si cette option est désactivée, aucun journal de requêtes Web n'est créé pour les tentatives d'accès au compartiment S3 identifié. Toutefois, les appels de l'API de gestion S3 au compartiment, par exemple [DeleteBucket](#), sont toujours suivis. Si la journalisation des événements de données S3 est activée CloudTrail pour ce compartiment, les requêtes Web pour les objets du compartiment seront toujours suivies. La désactivation de la journalisation est une technique utilisée par des utilisateurs non autorisés pour éviter la détection. Pour en savoir plus sur les journaux S3, veuillez consulter [Journalisation des accès au serveur S3](#) et [Options de journalisation S3](#) (langue française non garantie).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Une API S3 a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3, comme PutObject ou PutObjectAcl, a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

UnauthorizedAccess:S3/TorIPCaller

Une API S3 a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3, comme PutObject ou PutObjectAcl, a été invoquée depuis une adresse IP du nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cette découverte peut indiquer un accès non autorisé à vos AWS ressources dans le but de masquer la véritable identité de l'attaquant.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Types de recherche de protection EKS

Les résultats suivants sont spécifiques aux ressources Amazon EKS et ont un `resource_type` de `EKSCluster`. La gravité et les détails des résultats diffèrent selon le type de résultat.

Pour tous les résultats de type journaux d'audit EKS, nous vous recommandons d'examiner la ressource en question afin de déterminer si l'activité est attendue ou potentiellement malveillante. Pour obtenir des conseils sur la correction d'une ressource de journaux d'audit EKS compromise identifiée par une GuardDuty constatation, voir [Corriger les résultats de la protection EKS](#).

Note

Si l'activité à l'origine de ces résultats est attendue, envisagez d'ajouter [Règles de suppression dans GuardDuty](#) pour éviter de futures alertes.

Rubriques

- [CredentialAccess:Kubernetes/MaliciousIPCaller](#)
- [CredentialAccess:Kubernetes/MaliciousIPCaller.Custom](#)
- [CredentialAccess:Kubernetes/SuccessfulAnonymousAccess](#)
- [CredentialAccess:Kubernetes/TorIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom](#)
- [DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess](#)
- [DefenseEvasion:Kubernetes/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)

- [Impact:Kubernetes/MaliciousIPCaller](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Impact:Kubernetes/SuccessfulAnonymousAccess](#)
- [Impact:Kubernetes/TorIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/SuccessfulAnonymousAccess](#)
- [Persistence:Kubernetes/TorIPCaller](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- [CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated](#)
- [Execution:Kubernetes/AnomalousBehavior.ExecInPod](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer](#)
- [Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount](#)
- [Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated](#)
- [Discovery:Kubernetes/AnomalousBehavior.PermissionChecked](#)

Note

Avant la version 1.14 de Kubernetes, le `system:unauthenticated` groupe était associé à `system:discovery` et par défaut, `system:basic-user` ClusterRoles. Cette association peut autoriser un accès involontaire de la part d'utilisateurs anonymes. Les mises à jour du cluster ne révoquent pas ces autorisations. Même si vous avez mis à jour votre cluster vers la version 1.14 ou ultérieure, ces autorisations peuvent toujours être activées. Nous vous recommandons de dissocier ces autorisations du groupe `system:unauthenticated`. Pour obtenir des conseils sur la révocation de ces autorisations, consultez les [meilleures pratiques de sécurité pour Amazon EKS](#) dans le guide de l'utilisateur Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est

répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, le cas échéant, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) dans le guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'action d'API signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été

accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler les modifications apportées par un adversaire à votre cluster. Pour plus d'informations, consultez [Bonnes pratiques en matière de sécurité pour Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

CredentialAccess:Kubernetes/TorIPCaller

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée à partir d'une adresse IP de nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à vos ressources de cluster Kubernetes dans le but de masquer la véritable identité du pirate.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour contourner les mesures défensives a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer ses actions pour éviter d'être détecté.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour contourner les mesures défensives a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer ses actions pour éviter d'être détecté.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour contourner les mesures défensives a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer ses actions pour éviter d'être détecté. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'action d'API signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler les modifications apportées par un adversaire à votre cluster. Pour plus d'informations, consultez [Bonnes pratiques en matière de sécurité pour Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

DefenseEvasion:Kubernetes/TorIPCaller

Une API couramment utilisée pour contourner les mesures défensives a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer ses actions pour éviter d'être détecté. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à votre cluster Kubernetes dans le but de masquer la véritable identité de l'adversaire.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Discovery:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée à partir d'une adresse IP.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est couramment utilisée lors de la phase de

découverte d'une attaque au cours de laquelle un pirate collecte des informations pour déterminer si votre cluster Kubernetes est vulnérable à une attaque de plus grande envergure.

 Pour un accès non authentifié

MaliciousIPCallerles résultats ne sont pas générés pour un accès non authentifié.

SuccessfulAnonymousAccessles résultats sont générés pour un accès anonyme ou non authentifié.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Discovery:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une API a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'API observée est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un pirate collecte des informations pour déterminer si votre cluster Kubernetes est vulnérable à une attaque de plus grande envergure.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Discovery:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée à la phase de découverte d'une attaque lorsqu'un adversaire collecte des informations sur votre cluster Kubernetes. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'action d'API signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Ce type de recherche exclut les points de terminaison de l'API de contrôle de santé tels que `/healthz`, `/livez`, `/readyz`, et `/version`.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler les modifications apportées par un adversaire à votre cluster. Pour plus d'informations, consultez [Bonnes pratiques en matière de sécurité pour Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Discovery:Kubernetes/TorIPCaller

Une API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un pirate collecte des informations pour déterminer si votre cluster Kubernetes est vulnérable à une attaque de plus grande envergure. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à votre cluster Kubernetes dans le but de masquer la véritable identité de l'adversaire.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) dans le guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Execution:Kubernetes/ExecInKubeSystemPod

Une commande a été exécutée dans un pod au sein de l'espace de noms **kube-system**

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une commande a été exécutée dans un pod au sein de l'espace de noms kube-system à l'aide de l'API Kubernetes exec. L'espace de noms kube-system est un espace de noms par défaut, principalement utilisé pour les composants au niveau du système tels que kube-dns et kube-proxy. Il est très rare d'exécuter des commandes dans des pods ou des conteneurs situés sous un espace de noms kube-system, ce qui peut indiquer une activité suspecte.

Recommandations de correction :

Si l'exécution de cette commande est inattendue, les informations d'identification de l'utilisateur utilisées pour exécuter la commande peuvent être compromises. Révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Impact:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre AWS environnement.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Impact:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'API observée est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre AWS environnement.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Impact:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée à la phase d'impact d'une attaque lorsqu'un adversaire altère les ressources de votre cluster. Cette activité indique qu'un accès anonyme ou non authentifié

est autorisé sur l'action d'API signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler les modifications apportées par un adversaire à votre cluster. Pour plus d'informations, consultez [Bonnes pratiques en matière de sécurité pour Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Impact:Kubernetes/TorIPCaller

Une API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée à des tactiques d'impact où un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre environnement AWS . Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à votre cluster Kubernetes dans le but de masquer la véritable identité de l'adversaire.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez

l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Persistence:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour obtenir un accès permanent à un cluster Kubernetes a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de le conserver.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Persistence:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour obtenir un accès permanent à un cluster Kubernetes a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est

répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de le conserver.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Persistence:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour obtenir des autorisations de haut niveau sur un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée aux tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster et tente de le conserver. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'action d'API signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler les modifications apportées par un adversaire à votre cluster. Pour plus d'informations, consultez [Bonnes pratiques en matière de sécurité pour Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Persistence:Kubernetes/TorIPCaller

Une API couramment utilisée pour obtenir un accès permanent à un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de le conserver. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la section `KubernetesUserDetails` est `system:anonymous`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section [Bonnes pratiques de sécurité pour Amazon EKS](#) du Guide de l'utilisateur Amazon EKS. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Le compte de service par défaut a reçu des privilèges d'administrateur sur un cluster Kubernetes.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe que le compte de service par défaut pour un espace de noms de votre cluster Kubernetes a reçu des privilèges d'administrateur. Kubernetes crée un compte de service par défaut pour tous les espaces de noms du cluster. Il attribue automatiquement le compte de service par défaut en tant qu'identité aux pods qui n'ont pas été explicitement associés à un autre compte de service. Si le compte de service par défaut possède des privilèges d'administrateur, des pods peuvent être lancés involontairement avec des privilèges d'administrateur. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous ne devez pas utiliser le compte de service par défaut pour accorder des autorisations aux pods. Vous devez plutôt créer un compte de service dédié pour chaque charge de travail et accorder l'autorisation à ce compte en fonction des besoins. Pour résoudre ce problème, vous devez créer des comptes de service dédiés pour tous vos pods et charges de travail et mettre à jour les pods et les charges de travail afin d'effectuer une migration du compte de service par défaut vers leurs comptes dédiés. Vous devez ensuite supprimer l'autorisation d'administrateur du compte de service par défaut. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Policy:Kubernetes/AnonymousAccessGranted

L'utilisateur **system:anonymous** a obtenu l'autorisation d'API sur un cluster Kubernetes.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'un utilisateur de votre cluster Kubernetes est parvenu à créer une `ClusterRoleBinding` ou une `RoleBinding` pour lier l'utilisateur à un rôle `system:anonymous`. Cela permet un accès non authentifié aux opérations d'API autorisées par le rôle. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` ou au groupe `system:unauthenticated` de votre cluster et révoquer les accès anonymes inutiles. Pour plus

d'informations, consultez [Bonnes pratiques en matière de sécurité pour Amazon EKS](#) dans le Guide de l'utilisateur Amazon EKS. Si les autorisations ont été accordées de manière malveillante, vous devez révoquer l'accès de l'utilisateur qui les a accordées et annuler les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Policy:Kubernetes/ExposedDashboard

Le tableau de bord d'un cluster Kubernetes a été exposé sur Internet

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe que le tableau de bord Kubernetes de votre cluster a été exposé sur Internet par un service d'équilibreur de charge. Un tableau de bord exposé permet d'accéder à l'interface de gestion de votre cluster depuis Internet et permet aux adversaires d'exploiter les éventuelles failles d'authentification et de contrôle d'accès.

Recommandations de correction :

Vous devez vous assurer que l'authentification et l'autorisation fortes sont appliquées sur le tableau de bord Kubernetes. Vous devez également implémenter le contrôle d'accès au réseau pour restreindre l'accès au tableau de bord à partir d'adresses IP spécifiques.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Policy:Kubernetes/KubeflowDashboardExposed

Le Kubeflow le tableau de bord d'un cluster Kubernetes a été exposé à Internet

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe que le tableau de bord Kubeflow de votre cluster a été exposé sur Internet par un service d'équilibreur de charge. Un tableau de bord Kubeflow exposé permet d'accéder à l'interface de gestion de votre environnement Kubeflow depuis Internet et permet aux adversaires d'exploiter les éventuelles failles d'authentification et de contrôle d'accès.

Recommandations de correction :

Vous devez vous assurer que l'authentification et l'autorisation fortes sont appliquées sur le tableau de bord Kubeflow. Vous devez également implémenter le contrôle d'accès au réseau pour restreindre l'accès au tableau de bord à partir d'adresses IP spécifiques.

Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Une API Kubernetes couramment utilisée pour accéder aux secrets a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API anormale visant à récupérer des secrets de cluster sensibles a été invoquée par un utilisateur Kubernetes dans votre cluster. L'API observée est généralement associée à des tactiques d'accès aux informations d'identification qui peuvent entraîner une escalade des privilèges et un accès accru au sein de votre cluster. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification AWS sont compromises.

L'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster EKS et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle de ML suit plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations accordées à l'utilisateur Kubernetes dans votre cluster et assurez-vous que toutes ces autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Un rôle trop permissif RoleBinding ou ClusterRoleBinding un espace de noms sensible ont été créés ou modifiés dans votre cluster Kubernetes.

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si un RoleBinding ou ClusterRoleBinding implique le ClusterRoles admin ou cluster-admin, la gravité est élevée.

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'un utilisateur de votre cluster Kubernetes a créé une RoleBinding ou une ClusterRoleBinding pour lier un utilisateur à un rôle avec des autorisations d'administrateur ou des espaces de noms sensibles. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification AWS sont compromises.

L'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit aussi plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations accordées à l'utilisateur Kubernetes. Ces autorisations sont définies dans le rôle et les sujets concernés dans RoleBinding et ClusterRoleBinding. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez

les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Une commande a été exécutée à l'intérieur d'un pod de manière anormale.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une commande a été exécutée dans un pod à l'aide de l'API Kubernetes exec. L'API Kubernetes exec permet d'exécuter des commandes arbitraires dans un pod. Si ce comportement n'est pas attendu pour l'utilisateur, l'espace de noms ou le pod, cela peut indiquer une erreur de configuration ou que vos AWS informations d'identification sont compromises.

L'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit aussi plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si l'exécution de cette commande est inattendue, les informations d'identification de l'utilisateur utilisées pour exécuter la commande peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Une charge de travail a été lancée avec un conteneur privilégié de manière anormale.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une charge de travail a été lancée avec un conteneur privilégié dans votre cluster Amazon EKS. Un conteneur privilégié dispose d'un accès au niveau racine à l'hôte. Les utilisateurs non autorisés peuvent lancer des conteneurs privilégiés comme tactique d'escalade des privilèges pour d'abord accéder à l'hôte, puis le compromettre.

La création ou la modification du conteneur observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur et des images de conteneur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression avec des critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit avoir la même valeur que le champ

imagePrefix spécifié dans le résultat. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

Une charge de travail a été déployée de manière anormale, avec un chemin d'accès de l'hôte sensible installé à l'intérieur de la charge de travail.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une charge de travail a été lancée avec un conteneur qui incluait un chemin d'accès de l'hôte sensible dans la section volumeMounts. Cela rend potentiellement le chemin d'accès de l'hôte sensible accessible et inscriptible depuis l'intérieur du conteneur. Cette technique est couramment utilisée par des utilisateurs non autorisés pour accéder au système de fichiers de l'hôte.

La création ou la modification du conteneur observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur et des images de conteneur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression avec des critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit avoir la même valeur que le champ `imagePrefix` spécifié dans le résultat. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Une charge de travail a été lancée de manière anormale.

Gravité par défaut : faible*

Note

Le niveau de gravité par défaut est faible. Toutefois, si la charge de travail contient un nom d'image potentiellement suspect, tel qu'un outil pentest connu, ou si un conteneur exécute une commande potentiellement suspecte au lancement, telle que des commandes shell inverses, le niveau de gravité de ce type de résultat sera considéré comme moyen.

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une charge de travail Kubernetes a été créée ou modifiée de manière anormale, par exemple en raison d'une activité d'API, de nouvelles images de conteneur ou d'une configuration de charge de travail risquée, au sein de votre cluster Amazon EKS. Les utilisateurs non autorisés peuvent lancer des conteneurs comme tactique pour exécuter du code arbitraire pour d'abord accéder à l'hôte, puis le compromettre.

La création ou la modification du conteneur observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur et des images de conteneur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression avec des critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit avoir la même valeur que le champ `imagePrefix` spécifié dans le résultat. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Rôle hautement permissif ou ClusterRole créé ou modifié de manière anormale.

Gravité par défaut : faible

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API anormale visant à créer un `Role` ou un `ClusterRole` avec des autorisations excessives a été appelée par un utilisateur Kubernetes dans votre cluster Amazon EKS. Les acteurs peuvent utiliser la création de rôles avec de puissantes autorisations pour éviter d'utiliser des rôles intégrés de type administrateur et éviter d'être détectés. Les autorisations excessives peuvent entraîner une escalade des privilèges, l'exécution de code à distance et éventuellement le contrôle d'un espace de noms ou d'un cluster. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

L'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster Amazon EKS et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle de ML suit également plusieurs facteurs liés

au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations définies dans `Role` ou `ClusterRole` pour vous assurer que toutes les autorisations sont nécessaires et respectez le principe du moindre privilège. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un utilisateur a vérifié son autorisation d'accès de manière anormale.

Gravité par défaut : faible

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'un utilisateur de votre cluster Kubernetes est parvenu à vérifier si les puissantes autorisations connues pouvant entraîner une escalade des privilèges et l'exécution de code à distance sont autorisées ou non. Par exemple, une commande couramment utilisée pour vérifier les autorisations d'un utilisateur est `kubectl auth can-i`. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification ont été compromises.

L'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster Amazon EKS et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle de ML suit également plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'autorisation en cours de vérification et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations accordées à l'utilisateur Kubernetes pour vous assurer qu'elles sont toutes nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si vos AWS informations d'identification sont compromises, consultez [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

GuardDuty Types de recherche liés à la surveillance du temps

Amazon GuardDuty génère les résultats de surveillance du temps d'exécution suivants pour indiquer les menaces potentielles en fonction du comportement au niveau du système d'exploitation des hôtes et conteneurs Amazon EC2 dans vos clusters Amazon EKS, des charges de travail Fargate et Amazon ECS et des instances Amazon EC2.

GuardDuty génère certains types de recherche de surveillance du temps d'exécution uniquement lorsque vous activez les règles de détection personnalisées pour la surveillance du temps d'exécution. Pour ces types de recherche, voir [Recherche des types nécessitant des règles de détection personnalisées](#).

Note

Les types de résultat de la surveillance d'exécution sont basés sur les journaux d'exécution collectés auprès des hôtes. Les journaux contiennent des champs tels que les chemins d'accès aux fichiers qui peuvent être contrôlés par un acteur malveillant. Ces champs sont également inclus dans les GuardDuty résultats pour fournir un contexte d'exécution. Lorsque vous traitez les résultats de Runtime Monitoring en dehors de GuardDuty la console, vous devez nettoyer les champs de recherche. Par exemple, vous pouvez coder en HTML les champs de résultat lorsque vous les affichez sur une page Web.

Rubriques

- [Recherche des types générés par défaut par Runtime Monitoring](#)
- [Recherche des types nécessitant des règles de détection personnalisées](#)

Recherche des types générés par défaut par Runtime Monitoring

GuardDuty génère les types de recherche dans cette section lorsque vous activez la surveillance du temps d'exécution. Il n'est pas nécessaire d'activer les règles de détection personnalisées pour la surveillance du temps d'exécution pour obtenir ces types de résultats.

Rubriques

- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [UnauthorizedAccess:Runtime/TorRelay](#)
- [UnauthorizedAccess:Runtime/TorClient](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/DropPoint](#)
- [CryptoCurrency:Runtime/BitcoinTool.B! DNS](#)
- [Backdoor:Runtime/C&CActivity.B! DNS](#)
- [Trojan:Runtime/BlackholeTraffic! DNS](#)
- [Trojan:Runtime/DropPoint! DNS](#)
- [Trojan:Runtime/DGADomainRequest.C! DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic! DNS](#)
- [Trojan:Runtime/PhishingDomainRequest! DNS](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [DefenseEvasion:Runtime/ProcessInjection.Proc](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)

- [Execution:Runtime/ReverseShell](#)
- [DefenseEvasion:Runtime/FilelessExecution](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/MaliciousFileExecuted.Custom](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/KernelModuleLoaded](#)
- [Persistence:Runtime/SensitiveFileModified](#)
- [PrivilegeEscalation:Runtime/SensitiveFileModified](#)
- [DefenseEvasion:Runtime/SensitiveFileModified](#)

CryptoCurrency:Runtime/BitcoinTool.B

Une instance Amazon EC2 ou un conteneur interroge une adresse IP associée à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement interroge une adresse IP associée à une activité liée aux

cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si vous utilisez cette instance EC2 ou un conteneur pour exploiter ou gérer de la cryptomonnaie, ou si l'un d'eux est impliqué d'une autre manière dans une activité de blockchain, le résultat `CryptoCurrency:Runtime/BitcoinTool.B` peut représenter une activité attendue pour votre environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère de filtre doit utiliser l'attribut Type de résultat avec la valeur `CryptoCurrency:Runtime/BitcoinTool.B`. Le deuxième critère de filtre doit être l'ID d'instance de l'instance ou l'ID d'image de conteneur du conteneur impliqué dans une activité liée à la cryptomonnaie ou à la blockchain. Pour de plus amples informations, consultez [Règles de suppression](#).

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Backdoor:Runtime/C&CActivity.B

Une instance Amazon EC2 ou un conteneur interroge une adresse IP associée à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement interroge une adresse IP associée à un serveur de commande et de contrôle (C&C) connu. L'instance ou le conteneur répertorié est peut-être potentiellement compromis. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui sont infectés et contrôlés par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer une attaque par déni de service distribué (DDoS).

Note

Si l'adresse IP demandée est liée à log4j, les champs du résultat associé incluront les valeurs suivantes :

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

UnauthorizedAccess:Runtime/TorRelay

Votre instance Amazon EC2 ou un conteneur est en train de se connecter à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement établit des connexions à un réseau Tor d'une manière qui suggère qu'il agit comme un relais Tor. Tor est un logiciel permettant d'activer les communications

anonymes. Tor augmente l'anonymat de la communication en réacheminant le trafic potentiellement illicite du client d'un relais Tor à un autre.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

UnauthorizedAccess:Runtime/TorClient

Votre instance Amazon EC2 ou un conteneur est en train de se connecter à un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement établit des connexions à un nœud Tor Guard ou Authority. Tor est un logiciel permettant d'activer les communications anonymes. Les nœuds Tor Guards et Authority agissent en tant que passerelles initiales dans un réseau Tor. Ce trafic peut indiquer que cette instance EC2 ou le conteneur a été potentiellement compromis et agit en tant que client sur un réseau Tor. Cette découverte peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/BlackholeTraffic

Une instance Amazon EC2 ou un conteneur tente de communiquer avec une adresse IP d'un hôte distant qui est un trou noir connu.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement peut être compromis car il tente de communiquer avec l'adresse IP d'un trou noir (ou puits). Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire. Une adresse IP de trou noir désigne une machine hôte qui n'est pas en cours d'exécution ou une adresse à laquelle aucun hôte n'a été attribué.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/DropPoint

Une instance ou un conteneur Amazon EC2 tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement tente de communiquer avec l'adresse IP d'un hôte distant connu

pour détenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

CryptoCurrency:Runtime/BitcoinTool.B! DNS

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine associé à une activité de cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement interroge un nom de domaine associé à Bitcoin ou à une autre activité liée aux cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si vous utilisez cette instance EC2 ou un conteneur pour exploiter ou gérer de la cryptomonnaie, ou si l'un d'eux est impliqué d'une autre manière dans une activité de blockchain, le résultat CryptoCurrency:Runtime/BitcoinTool.B!DNS peut être une activité attendue pour votre

environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Le deuxième critère de filtre doit être l'ID d'instance de l'instance ou l'ID d'image de conteneur du conteneur impliqué dans une activité de cryptomonnaie ou de blockchain. Pour de plus amples informations, veuillez consulter [Règles de suppression](#).

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Backdoor:Runtime/C&CActivity.B!DNS

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine associé à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement interroge un nom de domaine associé à un serveur de commande et de contrôle (C&C) connu. L'instance EC2 ou le conteneur répertorié est peut-être compromis. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui sont infectés et contrôlés par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer une attaque par déni de service distribué (DDoS).

Note

Si le nom de domaine demandé est lié à log4j, les champs du résultat associé incluront les valeurs suivantes :

- `service.additionalInfo.threatListName = Amazon`

- `service.additionalInfo.threatName = Log4j Related`

Note

Pour tester le GuardDuty mode de génération de ce type de recherche, vous pouvez effectuer une requête DNS depuis votre instance `dig` (sous Linux ou `nslookup` Windows) sur un domaine de `testguarddutyactivityb.com`.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/BlackholeTraffic! DNS

Une instance Amazon EC2 ou un conteneur interroge le nom d'un domaine qui est redirigé vers l'adresse IP d'un trou noir.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement peut être compromis car il interroge un nom de domaine qui est redirigé vers une adresse IP de trou noir. Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des

informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/DropPoint! DNS

Une instance Amazon EC2 ou un conteneur interroge le nom de domaine d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement interroge le nom de domaine d'un hôte distant connu pour contenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/DGADomainRequest.C! DNS

Une instance Amazon EC2 ou un conteneur interroge des domaines générés par des algorithmes. Ces domaines sont couramment utilisés par des programmes malveillants et peuvent constituer une indication d'instance EC2 ou de conteneur compromis.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement tente d'interroger les domaines de l'algorithme de génération de domaines (DGA). Votre ressource a peut-être été compromise.

Ces algorithmes servent à générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle. Les serveurs de commande et de contrôle sont des ordinateurs qui émettent des commandes aux membres d'un botnet, qui est un ensemble d'appareils connectés à Internet qui sont infectés et contrôlés par un type courant de programme malveillant. Le grand nombre de points de rendez-vous potentiels rend l'arrêt des botnets difficile, car les ordinateurs infectés tentent de contacter certains de ces noms de domaine chaque jour pour recevoir des mises à jour ou des commandes.

 Note

Ce résultat est basé sur des domaines DGA connus issus de flux de renseignements sur les GuardDuty menaces.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/DriveBySourceTraffic! DNS

Une instance ou un conteneur Amazon EC2 interroge le nom de domaine d'un hôte distant qui est une source connue d'attaques par téléchargement. Drive-By

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus s'exécutant sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement peut être compromis car il interroge le nom de domaine

d'un hôte distant qui est une source connue d'attaques de téléchargement au volant. Il s'agit de téléchargements involontaires de logiciels d'Internet qui peuvent initier l'installation automatique de virus, logiciels espions ou programmes malveillants.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Trojan:Runtime/PhishingDomainRequest! DNS

Une instance Amazon EC2 ou un conteneur interroge des domaines impliqués dans des attaques d'hameçonnage.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement tente d'interroger un domaine impliqué dans des attaques de phishing. Les domaines de hameçonnage sont créés par des pirates se faisant passer pour une institution légitime afin de pousser des utilisateurs à fournir des données sensibles, telles que des informations personnelles identifiables, des coordonnées bancaires, des informations de carte bancaire ou des mots de passe. Votre instance EC2 ou le conteneur essaie peut-être de récupérer des données sensibles stockées sur un site Web d'hameçonnage ou d'en configurer un. Votre instance EC2 ou le conteneur pourrait être compromis.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Impact:Runtime/AbusedDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine de mauvaise réputation associé à des domaines abusifs connus.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP connus pour être utilisés de manière abusive. Les noms de domaine de premier niveau (TLD) et les noms de domaine de deuxième niveau (2LD) fournissant des enregistrements de sous-domaines gratuits ainsi que les fournisseurs de DNS dynamiques sont des exemples de domaines utilisés de manière abusive. Les acteurs de la menace ont tendance à utiliser ces services pour enregistrer des domaines gratuitement ou à faible coût. Les domaines de mauvaise réputation de cette catégorie peuvent également être des domaines expirés renvoyés à l'adresse IP de stationnement d'un bureau d'enregistrement et peuvent donc ne plus être actifs. Une adresse IP de stationnement est l'endroit où un bureau d'enregistrement dirige le trafic vers des domaines qui n'ont été liés à aucun service. L'instance Amazon EC2 répertoriée ou le conteneur peut être compromis, car les acteurs malveillants utilisent couramment ces bureaux d'enregistrement ou ces services pour la distribution de logiciels malveillants et de commande et de contrôle.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Impact:Runtime/BitcoinDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine de mauvaise réputation associé à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation associé à Bitcoin ou à une autre activité liée aux cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si vous utilisez cette instance EC2 ou le conteneur pour exploiter ou gérer de la cryptomonnaie, ou si ces ressources sont impliquées d'une autre manière dans une activité de blockchain, ce résultat peut représenter une activité attendue pour votre environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère de filtre doit utiliser l'attribut Type de résultat avec la valeur Impact:Runtime/BitcoinDomainRequest.Reputation. Le deuxième critère de filtre doit être l'ID d'instance de l'instance ou l'ID d'image de conteneur du conteneur impliqué dans une activité liée à la cryptomonnaie ou à la blockchain. Pour de plus amples informations, veuillez consulter [Règles de suppression](#).

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Impact:Runtime/MaliciousDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un de domaine de mauvaise réputation associé à des domaines malveillants connus.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP malveillants connus. Par exemple, les domaines peuvent être associés à une adresse IP de gouffre connue. Les domaines de gouffre sont des domaines qui étaient auparavant contrôlés par un acteur menaçant, et les demandes qui leur sont adressées peuvent indiquer que l'instance est compromise. Ces domaines peuvent également être corrélés à des campagnes malveillantes ou à des algorithmes de génération de domaines connus.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Impact:Runtime/SuspiciousDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine de mauvaise réputation qui est suspect par nature en raison de son ancienneté ou de sa faible popularité.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation soupçonné d'être malveillant. Les caractéristiques observées de ce domaine étaient cohérentes avec celles des domaines malveillants précédemment observés. Cependant, notre modèle de réputation n'était pas en mesure de le relier définitivement à une menace connue. Ces domaines sont généralement récemment observés ou reçoivent un faible trafic.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

UnauthorizedAccess:Runtime/MetadataDNSRebind

Une instance Amazon EC2 ou un conteneur effectue des recherches DNS résolues en service de métadonnées d'instance.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Note

Actuellement, ce type de recherche n'est pris en charge que pour l'architecture AMD64.

Ce résultat vous indique qu'un processus exécuté sur l'instance EC2 répertoriée ou sur un conteneur de votre AWS environnement interroge un domaine qui correspond à l'adresse IP des métadonnées EC2 (169.254.169.254). Une requête DNS de ce type peut indiquer que l'instance est une cible d'une technique de liaison DNS. Celle-ci qui peut être utilisée pour obtenir des métadonnées à partir d'une instance EC2, y compris les informations d'identification IAM associées à l'instance.

La liaison DNS implique de tromper une application s'exécutant sur l'instance EC2 pour charger des données de retour à partir d'une URL, où le nom de domaine de l'URL se résout en adresse IP des métadonnées EC2 (169.254.169.254). Cela conduit l'application à accéder aux métadonnées EC2 et éventuellement à les mettre à la disposition du pirate.

Il est possible d'accéder aux métadonnées EC2 à l'aide de la fonction de liaison DNS uniquement si l'instance EC2 exécute une application vulnérable qui permet l'injection d'URL, ou si une personne accède à l'URL dans un navigateur Web s'exécutant sur l'instance EC2.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

En réponse à ce résultat, vous devez évaluer s'il existe une application vulnérable en cours d'exécution sur l'instance EC2 ou le conteneur ou si une personne a utilisé un navigateur pour accéder au domaine identifié dans le résultat. Si la cause première est une application vulnérable, corrigez la vulnérabilité. Si une personne a navigué dans le domaine identifié, bloquez le domaine ou empêchez les utilisateurs d'y accéder. Si vous déterminez que ce résultat était lié à l'un ou l'autre des cas ci-dessus, [révoquez la session associée à l'instance EC2](#).

Certains AWS clients associent intentionnellement l'adresse IP des métadonnées à un nom de domaine sur leurs serveurs DNS officiels. Si c'est le cas dans votre environnement, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère de filtre doit utiliser l'attribut Type de résultat avec la valeur `UnauthorizedAccess:Runtime/MetadataDNSRebind`. Le deuxième critère de filtre doit être Domaine de demande DNS ou l'ID de l'image du conteneur. La valeur Domaine de demande DNS doit correspondre au domaine que vous avez mappé sur l'adresse IP des métadonnées (169.254.169.254). Pour plus d'informations sur la création de règles de suppression, veuillez consulter [Règles de suppression](#) (langue française non garantie).

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/NewBinaryExecuted

Un fichier binaire récemment créé ou modifié dans un conteneur a été exécuté.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un fichier binaire récemment créé ou récemment modifié dans un conteneur a été exécuté. Il est recommandé de conserver les conteneurs immuables au moment de l'exécution, et les fichiers binaires, les scripts ou les bibliothèques ne doivent pas être créés ou modifiés pendant la durée de vie du conteneur. Ce comportement indique qu'un acteur malveillant a potentiellement accédé au conteneur, a téléchargé et exécuté un logiciel malveillant ou un autre logiciel dans le cadre de la compromission potentielle. Bien que ce type d'activité puisse être le signe d'une violation, il s'agit également d'un modèle d'utilisation courant. Par conséquent, GuardDuty utilise des mécanismes pour identifier les instances suspectes de cette activité et génère ce type de recherche uniquement pour les instances suspectes.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Pour identifier le processus de modification et le nouveau binaire, consultez les détails du processus de modification et les détails du processus

Les détails du processus de modification sont inclus dans le `service.runtimeDetails.context.modifyingProcess` champ du JSON de recherche ou sous Processus de modification dans le panneau des détails de recherche. Pour ce type de recherche, le processus de modification est `/usr/bin/dpkg` défini par le `service.runtimeDetails.context.modifyingProcess.executablePath` champ du JSON de recherche ou fait partie du processus de modification dans le panneau des détails de la recherche.

Les détails du binaire nouveau ou modifié exécuté sont inclus dans le JSON `service.runtimeDetails.process` de recherche ou dans la section Processus sous Détails de l'exécution. Pour ce type de recherche, le binaire nouveau ou modifié est `/usr/bin/python3.8`, comme indiqué par le champ `service.runtimeDetails.process.executablePath` (Chemin exécutable).

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un processus à l'intérieur d'un conteneur communique avec le démon Docker à l'aide du socket Docker.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Le socket Docker est un socket de domaine Unix que le démon Docker (dockerd) utilise pour communiquer avec ses clients. Un client peut effectuer diverses actions, telles que la création de conteneurs en communiquant avec le démon Docker via le socket Docker. Il est suspect qu'un processus de conteneur accède au socket Docker. Un processus de conteneur peut échapper au conteneur et obtenir un accès au niveau de l'hôte en communiquant avec le socket Docker et en créant un conteneur privilégié.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/RuncContainerEscape

Une tentative d'échappement de conteneur via runC a été détectée.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

RunC est le runtime de conteneur de bas niveau que les environnements d'exécution de conteneurs de haut niveau, tels que Docker et Containerd, utilisent pour générer et exécuter des conteneurs. RunC est toujours exécuté avec les privilèges root car il doit effectuer la tâche de bas niveau consistant à créer un conteneur. Un acteur malveillant peut obtenir un accès au niveau de l'hôte en modifiant ou en exploitant une vulnérabilité dans le binaire RunC.

Cette découverte détecte la modification du binaire RunC et les tentatives potentielles d'exploitation des vulnérabilités RunC suivantes :

- [CVE-2019-5736](#)— L'exploitation de CVE-2019-5736 implique le remplacement du binaire RunC depuis un conteneur. Ce résultat est invoqué lorsque le binaire RunC est modifié par un processus à l'intérieur d'un conteneur.
- [CVE-2024-21626](#)— L'exploitation de CVE-2024-21626 implique de définir le répertoire de travail actuel (CWD) ou un conteneur sur un descripteur `/proc/self/fd/FileDescriptor` de fichier ouvert. Ce résultat est invoqué lorsqu'un processus conteneur contenant un répertoire de travail actuel `/proc/self/fd/` est détecté, par exemple `/proc/self/fd/7`.

Cette découverte peut indiquer qu'un acteur malveillant a tenté d'exploiter l'un des types de conteneurs suivants :

- Un nouveau conteneur avec une image contrôlée par un pirate.
- Conteneur existant accessible à l'acteur avec des autorisations d'écriture sur le binaire runC au niveau de l'hôte.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Une tentative d'échappement de conteneur via l'agent de libération CGroups a été détectée.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe qu'une tentative de modification du fichier de l'agent de version d'un groupe de contrôle (cgroup) a été détectée. Linux utilise des groupes de contrôle (cgroups) pour limiter, prendre en compte et isoler l'utilisation des ressources d'un ensemble de processus. Chaque cgroup

possède un fichier d'agent de version (`release_agent`), un script que Linux exécute lorsqu'un processus au sein du cgroup se termine. Le fichier de l'agent de version est toujours exécuté au niveau de l'hôte. Un acteur malveillant à l'intérieur d'un conteneur peut s'échapper vers l'hôte en écrivant des commandes arbitraires dans le fichier de l'agent de version qui appartient à un cgroup. Lorsqu'un processus à l'intérieur de ce cgroup se termine, les commandes écrites par l'acteur sont exécutées.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/ProcessInjection.Proc

Une injection de processus utilisant le système de fichiers `proc` a été détectée dans un conteneur ou une instance Amazon EC2.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

L'injection de processus est une technique utilisée par les acteurs malveillants pour injecter du code dans les processus afin d'échapper aux défenses et d'augmenter potentiellement les privilèges. Le système de fichiers `proc` (`procfs`) est un système de fichiers spécial sous Linux qui présente la mémoire virtuelle du processus sous forme de fichier. Le chemin de ce fichier est `/proc/PID/mem`, où `PID` est l'ID unique du processus. Un acteur malveillant peut écrire dans ce fichier pour injecter du code dans le processus. Ce résultat identifie les tentatives potentielles d'écriture dans ce fichier.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Une injection de processus utilisant un appel système ptrace a été détectée dans un conteneur ou une instance Amazon EC2.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

L'injection de processus est une technique utilisée par les acteurs malveillants pour injecter du code dans les processus afin d'échapper aux défenses et d'augmenter potentiellement les privilèges. Un processus peut utiliser l'appel système ptrace pour injecter du code dans un autre processus. Ce résultat identifie une tentative potentielle d'injection de code dans un processus à l'aide de l'appel système ptrace.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Une injection de processus via une écriture directe dans la mémoire virtuelle a été détectée dans un conteneur ou une instance Amazon EC2.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

L'injection de processus est une technique utilisée par les acteurs malveillants pour injecter du code dans les processus afin d'échapper aux défenses et d'augmenter potentiellement les privilèges. Un

processus peut utiliser un appel système, comme `process_vm_writev`, pour injecter directement du code dans la mémoire virtuelle d'un autre processus. Ce résultat identifie une tentative potentielle d'injection de code dans un processus à l'aide d'un appel système pour écrire dans la mémoire virtuelle du processus.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/ReverseShell

Un processus dans un conteneur ou une instance Amazon EC2 a créé un shell inversé.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Un shell inversé est une session shell créée sur une connexion initiée entre l'hôte cible et l'hôte de l'acteur. C'est le contraire d'un shell normal initié depuis l'hôte de l'acteur vers l'hôte de la cible. Les acteurs malveillants créent un shell inversé pour exécuter des commandes sur la cible après avoir obtenu un accès initial à celle-ci. Cette découverte identifie les connexions inverses Shell potentiellement suspectes.

GuardDuty examine l'activité d'exécution et le contexte associés, et génère ce type de recherche uniquement lorsque l'activité et le contexte associés s'avèrent inhabituels ou suspects. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

L'agent GuardDuty de sécurité surveille les événements provenant de sources multiples. Pour identifier la ressource affectée, consultez le type de ressource dans les informations de recherche de la GuardDuty console. Si cette activité est inattendue, votre type de ressource a peut-être

été compromis. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/FilelessExecution

Un processus dans un conteneur ou une instance Amazon EC2 exécute du code depuis la mémoire.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe lorsqu'un processus est exécuté à l'aide d'un fichier exécutable en mémoire sur le disque. Il s'agit d'une technique de contournement de la défense courante qui évite d'écrire le fichier exécutable malveillant sur le disque pour échapper à la détection basée sur l'analyse du système de fichiers. Bien que cette technique soit utilisée par des logiciels malveillants, elle présente également des cas d'utilisation légitimes. L'un des exemples est un compilateur juste-à-temps (JIT) qui écrit le code compilé dans la mémoire et l'exécute à partir de la mémoire.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Impact:Runtime/CryptoMinerExecuted

Un conteneur ou une instance Amazon EC2 exécute un fichier binaire associé à une activité d'exploitation de cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance ou le conteneur EC2 répertorié dans votre AWS environnement exécute un fichier binaire associé à une activité d'extraction de

cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console et consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/NewLibraryLoaded

Une bibliothèque récemment créée ou modifiée a été chargée par un processus à l'intérieur d'un conteneur.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat indique qu'une bibliothèque a été créée ou modifiée dans un conteneur pendant l'exécution et chargée par un processus exécuté dans le conteneur. Il est recommandé de conserver les conteneurs immuables au moment de l'exécution, et à ne pas créer ou modifier les fichiers binaires, les scripts ou les bibliothèques pendant la durée de vie du conteneur. Le chargement d'une bibliothèque récemment créée ou modifiée dans un conteneur peut indiquer une activité suspecte. Ce comportement indique qu'un acteur malveillant a potentiellement accédé au conteneur, a téléchargé et exécuté un logiciel malveillant ou un autre logiciel dans le cadre de la compromission potentielle. Bien que ce type d'activité puisse être le signe d'une violation, il s'agit également d'un modèle d'utilisation courant. Par conséquent, GuardDuty utilise des mécanismes pour identifier les instances suspectes de cette activité et génère ce type de recherche uniquement pour les instances suspectes.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un processus à l'intérieur d'un conteneur a monté un système de fichiers hôte au moment de l'exécution.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Plusieurs techniques de fuite de conteneur impliquent le montage d'un système de fichiers hôte dans un conteneur lors de l'exécution. Ce résultat indique qu'un processus à l'intérieur d'un conteneur a potentiellement tenté de monter un système de fichiers hôte, ce qui peut indiquer une tentative de fuite vers l'hôte.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un processus a utilisé les appels système **userfaultfd** pour traiter les erreurs de page dans l'espace utilisateur.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Généralement, les erreurs de page sont gérées par le noyau dans l'espace du noyau. Cependant, l'appel système **userfaultfd** permet à un processus de gérer les erreurs de page sur un système

de fichiers dans l'espace utilisateur. Il s'agit d'une fonctionnalité utile qui permet d'implémenter des systèmes de fichiers de l'espace utilisateur. D'autre part, il peut également être utilisé par un processus potentiellement malveillant pour interrompre le noyau depuis l'espace utilisateur. L'interruption du noyau à l'aide d'un appel système `userfaultfd` est une technique d'exploitation courante pour étendre les fenêtres de course pendant l'exploitation des conditions de course du noyau. L'utilisation de `userfaultfd` peut indiquer une activité suspecte sur l'instance Amazon Elastic Compute Cloud (Amazon EC2).

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/SuspiciousTool

Un conteneur ou une instance Amazon EC2 exécute un fichier binaire ou un script fréquemment utilisé dans des scénarios de sécurité offensifs tels que l'engagement des tests de pénétration.

Gravité par défaut : variable

La gravité de cette constatation peut être élevée ou faible, selon que l'outil suspect détecté est considéré comme étant à double usage ou s'il est exclusivement destiné à un usage offensif.

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un outil suspect a été exécuté sur une instance ou un conteneur EC2 au sein de votre AWS environnement. Cela inclut les outils utilisés dans les engagements de tests de pénétration, également appelés outils de porte dérobée, scanners réseau et détecteurs de réseau. Tous ces outils peuvent être utilisés dans des contextes bénins, mais ils sont également fréquemment utilisés par des acteurs malveillants à des fins malveillantes. L'observation d'outils de sécurité offensifs peut indiquer que l'instance ou le conteneur EC2 associé a été compromis.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/SuspiciousCommand

Une commande suspecte a été exécutée sur une instance Amazon EC2 ou un conteneur, ce qui indique une compromission.

Gravité par défaut : variable

En fonction de l'impact du modèle malveillant observé, la gravité de ce type de découverte peut être faible, moyenne ou élevée.

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une commande suspecte a été exécutée et qu'une instance Amazon EC2 ou un conteneur de votre AWS environnement a été compromis. Cela peut signifier qu'un fichier a été téléchargé à partir d'une source suspecte puis exécuté, ou qu'un processus en cours affiche un schéma malveillant connu dans sa ligne de commande. Cela indique en outre qu'un logiciel malveillant est en cours d'exécution sur le système.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

 Note

Les arguments de la ligne de commande du processus peuvent contenir des données sensibles. Pour protéger les données sensibles, les résultats de la surveillance de l' GuardDuty exécution n'incluent pas les arguments complets de la ligne de commande. `Service.RuntimeDetails.Context.CommandLineExample` fournit plutôt un exemple représentatif du modèle de ligne de commande qui a généré le résultat.

DefenseEvasion:Runtime/SuspiciousCommand

Une commande a été exécutée sur l'instance Amazon EC2 répertoriée ou sur un conteneur, elle tente de modifier ou de désactiver un mécanisme de défense Linux, tel qu'un pare-feu ou des services système essentiels.

Gravité par défaut : variable

Selon le mécanisme de défense qui a été modifié ou désactivé, la gravité de ce type de découverte peut être élevée, moyenne ou faible.

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'une commande visant à dissimuler une attaque des services de sécurité du système local a été exécutée. Cela inclut des actions telles que la désactivation du pare-feu Unix, la modification des tables IP locales, la suppression d'entrées crontab, la désactivation d'un service local ou la reprise de la fonction `LDPreload`. Toute modification est très suspecte et constitue un indicateur potentiel de compromission. Par conséquent, ces mécanismes détectent ou empêchent toute nouvelle compromission du système.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des

informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/PtraceAntiDebugging

Un processus d'un conteneur ou d'une instance Amazon EC2 a exécuté une mesure anti-débogage à l'aide de l'appel système ptrace.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat indique qu'un processus exécuté sur l'instance Amazon EC2 répertoriée ou sur un conteneur de votre AWS environnement a utilisé l'appel système ptrace avec l'option.

PTRACE_TRACEME Cette activité provoquerait le détachement d'un débogueur du processus en cours d'exécution. Si aucun débogueur n'est connecté, cela n'a aucun effet. Cependant, l'activité en elle-même éveille des soupçons. Cela peut indiquer qu'un logiciel malveillant est en cours d'exécution sur le système. Les logiciels malveillants utilisent fréquemment des techniques anti-débogage pour échapper à l'analyse et ces techniques peuvent être détectées lors de l'exécution.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/MaliciousFileExecuted

Un fichier exécutable malveillant connu a été exécuté sur une instance Amazon EC2 ou un conteneur.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un exécutable malveillant connu a été exécuté sur une instance Amazon EC2 ou un conteneur au sein de votre AWS environnement. Il s'agit d'un indicateur fort que l'instance ou le conteneur a été potentiellement compromis et qu'un logiciel malveillant a été exécuté.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/MaliciousFileExecuted.Custom

Un fichier exécutable malveillant connu a été exécuté sur une instance Amazon EC2 ou un conteneur.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un fichier exécutable inclus dans une liste d'entités de menace que vous avez chargée et activée a été exécuté sur une instance Amazon EC2 ou un conteneur au sein de votre AWS environnement. Dans GuardDuty, une liste d'entités de menace peut inclure des adresses

IP, des domaines et des hachages de SHA-256 fichiers malveillants connus. GuardDuty génère des résultats en fonction de l'activité associée à la liste d'entités de menace téléchargée. Vous pouvez consulter le nom de cette liste d'entités de menaces dans les détails du résultat.

Remarque : Ce résultat ne se déclenche que lorsqu'un fichier exécutable, dont le hachage a été inclus dans la liste des entités de menace, est exécuté.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Execution:Runtime/SuspiciousShellCreated

Un service réseau ou un processus accessible par le réseau sur une instance Amazon EC2 ou dans un conteneur a lancé un processus shell interactif.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un service accessible par le réseau sur une instance Amazon EC2 ou dans un conteneur au sein de AWS votre environnement a lancé un shell interactif. Dans certaines circonstances, ce scénario peut indiquer un comportement post-exploitation. Les shells interactifs permettent aux attaquants d'exécuter des commandes arbitraires sur une instance ou un conteneur compromis.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie. Vous pouvez voir les informations de processus accessibles par le réseau dans les détails du processus parent.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/ElevationToRoot

Un processus exécuté sur l'instance ou le conteneur Amazon EC2 répertorié a assumé les privilèges root.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'Amazon EC2 répertorié ou dans le conteneur répertorié au sein de votre AWS environnement a acquis les privilèges root suite à une exécution `setuid` binaire inhabituelle ou suspecte. Cela indique qu'un processus en cours d'exécution a été potentiellement compromis, pour l'instance EC2 par un exploit ou par une `setuid` exploitation. En utilisant les privilèges root, l'attaquant peut potentiellement exécuter des commandes sur l'instance ou le conteneur.

Bien qu' GuardDuty il soit conçu pour ne pas générer ce type de constatation pour les activités impliquant une utilisation régulière de la `sudo` commande, il génère ce résultat lorsqu'il identifie l'activité comme inhabituelle ou suspecte.

GuardDuty examine l'activité et le contexte d'exécution associés, et génère ce type de recherche uniquement lorsque l'activité et le contexte associés sont inhabituels ou suspects.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Discovery:Runtime/SuspiciousCommand

Une commande suspecte a été exécutée sur une instance Amazon EC2 ou dans un conteneur, ce qui permet à un attaquant d'obtenir des informations sur le système local, les environs AWS infrastructure, ou infrastructure de conteneurs.

Gravité par défaut : faible

Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance ou le conteneur Amazon EC2 répertorié dans votre AWS environnement a exécuté une commande susceptible de fournir à un attaquant des informations cruciales susceptibles de faire avancer l'attaque. Les informations suivantes ont peut-être été récupérées :

- Système local tel que la configuration utilisateur ou réseau,
- Autres AWS ressources et autorisations disponibles, ou
- Infrastructure Kubernetes, comme les services et les pods.

L'instance Amazon EC2 ou le conteneur répertorié dans les informations de recherche ont peut-être été compromis.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Vous pouvez trouver les détails de la commande suspecte dans le champ `service.runtimeDetails.context` du JSON de résultat. Un contexte supplémentaire, y compris des informations sur le processus et le lignage des processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Persistence:Runtime/SuspiciousCommand

Une commande suspecte a été exécutée sur une instance Amazon EC2 ou dans un conteneur, ce qui permet à un attaquant de conserver l'accès et le contrôle sur votre AWS environnement.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance Amazon EC2 répertoriée ou dans un conteneur de votre AWS environnement a exécuté une commande suspecte. La commande installe une méthode de persistance qui permet à un logiciel malveillant de s'exécuter sans interruption ou à un attaquant d'accéder en permanence à l'instance ou au type de ressource de conteneur potentiellement compromis. Cela peut signifier qu'un service système a été installé ou modifié, qu'il `crontab` a été modifié ou qu'un nouvel utilisateur a été ajouté à la configuration du système.

GuardDuty examine l'activité et le contexte d'exécution associés, et génère ce type de recherche uniquement lorsque l'activité et le contexte associés sont inhabituels ou suspects.

L'instance Amazon EC2 ou le conteneur répertorié dans les informations de recherche ont peut-être été compromis.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Vous pouvez trouver les détails de la commande suspecte dans le champ `service.runtimeDetails.context` du JSON de résultat. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/SuspiciousCommand

Une commande suspecte a été exécutée sur une instance Amazon EC2 ou dans un conteneur, ce qui permet à un attaquant d'augmenter ses privilèges.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur l'instance Amazon EC2 répertoriée ou dans un conteneur de votre AWS environnement a exécuté une commande suspecte. La commande tente d'augmenter les privilèges, ce qui permet à un adversaire d'exécuter des tâches à privilèges élevés.

GuardDuty examine l'activité et le contexte d'exécution associés, et génère ce type de recherche uniquement lorsque l'activité et le contexte associés sont inhabituels ou suspects.

L'instance Amazon EC2 ou le conteneur répertorié dans les informations de recherche ont peut-être été compromis.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/KernelModuleLoaded

Un module noyau a été chargé sur une instance Amazon EC2, ce qui indique une tentative d'accès au niveau du noyau.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat indique qu'un module de noyau a été chargé sur l'instance EC2 répertoriée. Étant donné que les modules du noyau ont les privilèges les plus élevés au niveau du système (anneau 0), cela peut indiquer qu'un acteur malveillant a obtenu un accès au niveau du noyau. Ce niveau d'accès permet un contrôle complet du système.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Le cas échéant, un contexte supplémentaire, y compris des informations sur le processus et le lignage du processus, est disponible dans les conclusions pour une enquête plus approfondie.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Persistence:Runtime/SensitiveFileModified

Un fichier système sensible a été modifié sur un conteneur ou une instance Amazon EC2, ce qui peut potentiellement permettre à un adversaire d'obtenir une persistance.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un fichier système sensible a été modifié sur un conteneur ou une instance Amazon EC2, ce qui peut potentiellement permettre à un adversaire d'obtenir des droits d'exécution persistants sur le système. Cela peut inclure l'installation de nouveaux fichiers clés SSH, des modifications des fichiers de configuration utilisateur, des modifications des fichiers de mots de passe ou des fichiers fantômes, la création de tâches planifiées, la manipulation de scripts de démarrage du système ou la modification de fichiers exécutables ou de scripts par des processus de service Web dans des contextes suspects. Ces modifications sont des indicateurs de compromission susceptibles de permettre une persistance non autorisée dans votre environnement.

GuardDuty surveille les fichiers système sensibles à la sécurité fréquemment ciblés par les adversaires pour garantir leur persistance. Étant donné que ces fichiers peuvent également être modifiés au cours de l'administration et de la gestion légitimes du système, GuardDuty examine l'activité d'exécution et le contexte associés pour générer ce résultat uniquement lorsque les modifications sont corrélées à d'autres activités suspectes.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Le champ `service.runtimeDetails.context` contient des informations sur la modification suspecte du fichier, notamment le chemin du fichier et le type d'opération.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

PrivilegeEscalation:Runtime/SensitiveFileModified

Un fichier système sensible a été modifié sur un conteneur ou une instance Amazon EC2, ce qui peut potentiellement permettre à un adversaire d'augmenter ses privilèges.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un fichier système sensible a été modifié sur un conteneur ou une instance Amazon EC2, ce qui peut potentiellement permettre à un adversaire d'augmenter ses privilèges sur le système. Cela peut impliquer des modifications de fichiers critiques pour la sécurité tels que la configuration de sudoers, les paramètres PAM ou les fichiers d'authentification du système. Ces modifications sont des indicateurs de compromission susceptibles de permettre une élévation de privilèges non autorisée, ce qui peut entraîner un accès root non autorisé, des mécanismes d'authentification affaiblis ou des contrôles de sécurité compromis.

GuardDuty surveille les fichiers système sensibles à la sécurité fréquemment ciblés par les adversaires pour l'augmentation des privilèges. Étant donné que ces fichiers peuvent également être modifiés au cours de l'administration et de la gestion légitimes du système, GuardDuty examine l'activité d'exécution et le contexte associés pour générer ce résultat uniquement lorsque les modifications sont corrélées à d'autres activités suspectes.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Le champ `service.runtimeDetails.context` contient des informations sur la modification suspecte du fichier, notamment le chemin du fichier et le type d'opération.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

DefenseEvasion:Runtime/SensitiveFileModified

Un fichier système sensible a été modifié sur un conteneur ou une instance Amazon EC2, ce qui peut potentiellement permettre à un adversaire d'échapper à la détection.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un fichier système sensible a été modifié sur un conteneur ou une instance Amazon EC2, ce qui peut potentiellement permettre à un adversaire d'échapper à la détection sur le système. Cela peut impliquer des modifications des fichiers journaux du système, des configurations d'audit, des fichiers d'historique des commandes ou des journaux système. Ces modifications sont des indicateurs de compromission susceptibles de permettre de dissimuler des activités non autorisées, de perturber la surveillance de la sécurité ou de supprimer des preuves de l'activité du système.

GuardDuty surveille les fichiers système sensibles à la sécurité fréquemment ciblés par les adversaires pour échapper à la défense. Étant donné que ces fichiers peuvent également être modifiés au cours de l'administration et de la gestion légitimes du système, GuardDuty examine l'activité d'exécution et le contexte associés pour générer ce résultat uniquement lorsque les modifications sont corrélées à d'autres activités suspectes.

L'agent GuardDuty d'exécution surveille les événements provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console. Le champ `service.runtimeDetails.context` contient des informations sur la modification suspecte du fichier, notamment le chemin du fichier et le type d'opération.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Recherche des types nécessitant des règles de détection personnalisées

GuardDuty génère les types de recherche suivants uniquement lorsque vous activez les règles de détection personnalisées pour la surveillance du temps d'exécution. Pour plus d'informations, consultez [Règles de détection personnalisées dans GuardDuty](#).

Chaque résultat inclut le `CustomDetectionRuleName` champ, qui contient le nom de la règle qui a généré le résultat.

Rubriques

- [CommandAndControl:Runtime/SuspiciousCommand](#)
- [CredentialAccess:Runtime/SensitiveFileRead](#)

- [Discovery:Runtime/SensitiveFileRead](#)
- [Exfiltration:Runtime/SuspiciousCommand](#)

CommandAndControl:Runtime/SuspiciousCommand

Un processus sur une instance Amazon EC2 ou dans un conteneur a exécuté une commande suspecte qu'un attaquant pourrait utiliser pour communiquer avec la ressource et la contrôler.

Gravité par défaut : variable

La gravité dépend de la règle qui a généré le résultat : élevée pour [DnsTunnelingToolExecuted](#) et moyenne pour [SuspiciousProtocolTunneling](#).

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus sur une instance ou un conteneur Amazon EC2 de votre AWS environnement a exécuté une commande qu'un attaquant pourrait utiliser pour communiquer avec une ressource compromise tout en évitant d'être détecté. Par exemple, le processus peut avoir exécuté un outil qui canalise le trafic via le DNS ou qui expose la ressource via un tunnel ou un service proxy.

GuardDuty génère ce résultat à partir des [SuspiciousProtocolTunneling](#) règles [DnsTunnelingToolExecuted](#) et.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

CredentialAccess:Runtime/SensitiveFileRead

Un processus sur une instance Amazon EC2 ou dans un conteneur a accédé à un fichier sensible susceptible de contenir des informations d'identification.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus sur une instance ou un conteneur Amazon EC2 de votre AWS environnement a accédé à un fichier sensible à la sécurité susceptible de contenir des

informations d'identification ou d'autres secrets. Par exemple, le processus peut avoir accédé à la mémoire d'un autre processus via le système de /proc fichiers pour en extraire les informations d'identification.

GuardDuty génère ce résultat à partir de la [DumpProcessMemoryFromProc](#) règle.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Discovery:Runtime/SensitiveFileRead

Un processus sur une instance Amazon EC2 ou dans un conteneur a accédé à un fichier sensible contenant des informations sur les utilisateurs locaux et les informations d'identification.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus sur une instance ou un conteneur Amazon EC2 de votre AWS environnement a accédé à un fichier système sensible à la sécurité, tel que le compte utilisateur local ou les fichiers de hachage des mots de passe. Un attaquant peut utiliser ces informations pour découvrir des comptes et tenter de déchiffrer leurs mots de passe.

GuardDuty génère ce résultat à partir de la [PasswordShadowFileDiscovery](#) règle.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Exfiltration:Runtime/SuspiciousCommand

Un processus sur une instance Amazon EC2 ou dans un conteneur a exécuté une commande suspecte qu'un attaquant pourrait utiliser pour déplacer des données hors de votre environnement.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus sur une instance ou un conteneur Amazon EC2 de votre AWS environnement a exécuté une commande susceptible d'être utilisée pour déplacer des données hors de votre environnement. Par exemple, le processus peut avoir chargé un fichier sur un point de terminaison externe ou un service de stockage dans le cloud, ou avoir divisé les données en plusieurs parties plus petites pour éviter les limites de transfert.

GuardDuty génère ce résultat à partir [CurlWgetExfiltrateData](#) des [S3DataExfiltrationWithRclone](#) règles [DataSplittingForExfiltration](#), et.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour plus d'informations, consultez [Correction des résultats de la surveillance d'exécution](#).

Protection contre les programmes malveillants pour les types de détection EC2

GuardDuty Malware Protection for EC2 fournit une protection antimalware unique permettant à EC2 de détecter toutes les menaces détectées lors de l'analyse d'une instance EC2 ou d'une charge de travail de conteneur. Le résultat inclut le nombre total de détections effectuées pendant l'analyse et, en fonction de leur gravité, fournit des détails sur les 32 principales menaces détectées. Contrairement à d'autres GuardDuty résultats, les résultats de Malware Protection for EC2 ne sont pas mis à jour lorsque la même instance EC2 ou la même charge de travail de conteneur est à nouveau analysée.

Une nouvelle protection contre les programmes malveillants détectée par EC2 est générée pour chaque analyse qui détecte un logiciel malveillant. Les résultats de la protection contre les programmes malveillants pour EC2 incluent des informations sur le scan correspondant à l'origine du résultat ainsi que sur le GuardDuty résultat à l'origine de ce scan. Il est ainsi plus facile de corréler le comportement suspect avec le logiciel malveillant détecté.

Note

Lorsqu'une activité malveillante est GuardDuty détectée sur une charge de travail de conteneur, Malware Protection for EC2 ne génère aucun résultat de niveau EC2.

Les résultats suivants concernent spécifiquement la protection contre les GuardDuty logiciels malveillants pour EC2.

Rubriques

- [Execution:EC2/MaliciousFile](#)
- [Execution:ECS/MaliciousFile](#)
- [Execution:Kubernetes/MaliciousFile](#)
- [Execution:Container/MaliciousFile](#)
- [Execution:EC2/SuspiciousFile](#)
- [Execution:ECS/SuspiciousFile](#)
- [Execution:Kubernetes/SuspiciousFile](#)
- [Execution:Container/SuspiciousFile](#)

Execution:EC2/MaliciousFile

Un fichier malveillant a été détecté sur une instance EC2.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur l'instance EC2 répertoriée dans votre AWS environnement. Cette instance répertoriée est peut-être compromise. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Execution:ECS/MaliciousFile

Un fichier malveillant a été détecté sur un cluster ECS.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur un workload de conteneur appartenant à un cluster ECS. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est inattendue, votre conteneur appartenant au cluster ECS peut être compromis. Pour de plus amples informations, veuillez consulter [Remédier à un cluster ECS potentiellement compromis](#).

Execution:Kubernetes/MaliciousFile

Un fichier malveillant a été détecté sur un cluster Kubernetes.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur un workload de conteneur appartenant à un cluster Kubernetes. S'il s'agit d'un cluster géré par EKS, les détails des résultats fourniront des informations supplémentaires sur la ressource EKS affectée. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Execution:Container/MaliciousFile

Un fichier malveillant a été détecté sur un conteneur autonome.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur un workload de conteneur et qu'aucune information sur le cluster n'a été

identifiée. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour de plus amples informations, veuillez consulter [Remédier à un conteneur autonome potentiellement compromis](#).

Execution:EC2/SuspiciousFile

Un fichier suspect a été détecté sur une instance EC2.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur une instance EC2. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type SuspiciousFile indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Execution:ECS/SuspiciousFile

Un fichier suspect a été détecté sur un cluster ECS.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur un conteneur appartenant à un cluster ECS. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est inattendue, votre conteneur appartenant au cluster ECS peut être compromis. Pour de plus amples informations, veuillez consulter [Remédier à un cluster ECS potentiellement compromis](#).

Execution:Kubernetes/SuspiciousFile

Un fichier suspect a été détecté sur un cluster Kubernetes.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur un conteneur appartenant à un cluster Kubernetes. S'il s'agit d'un cluster géré

par EKS, les détails des résultats fourniront des informations supplémentaires sur le service EKS concerné. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Execution:Container/SuspiciousFile

Un fichier suspect a été détecté sur un conteneur autonome.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur un conteneur sans aucune information sur le cluster. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour de plus amples informations, veuillez consulter [Remédier à un conteneur autonome potentiellement compromis](#).

Protection contre les programmes malveillants pour le type de recherche S3

GuardDuty génère un résultat uniquement lorsqu'il détecte une menace potentielle pour votre sécurité Compte AWS. Une détection de Malware Protection for S3 indique que l'objet chargé à l'origine de l'analyse des programmes malveillants contient un fichier potentiellement malveillant.

Pour GuardDuty qu'Amazon génère un résultat dans votre compte Compte AWS, activez à la fois la protection contre GuardDuty les logiciels malveillants pour S3. La meilleure pratique consiste d'abord à activer GuardDuty puis à activer la protection contre les programmes malveillants pour S3. Si cet ordre est différent pour vous, assurez-vous de l'activer GuardDuty avant qu'un objet S3 ne soit chargé dans votre compartiment protégé.

Note

GuardDuty Impossible de générer une recherche pour un objet S3 qui a été scanné avant l'activation GuardDuty. Pour scanner un objet S3 existant, vous pouvez le télécharger à nouveau.

Object:S3/MaliciousFile

Un fichier malveillant a été détecté sur un objet S3 scanné.

Gravité par défaut : élevée

- Fonctionnalité : Protection contre les logiciels malveillants pour S3

Cette découverte indique qu'une analyse des programmes malveillants a détecté que l'objet S3 répertorié était malveillant. Pour plus d'informations, consultez la section Menaces détectées dans le panneau des détails de la recherche.

Correction des recommandations :

Si cette découverte était inattendue, l'objet S3 est potentiellement malveillant. Pour plus d'informations sur les étapes de correction recommandées, consultez [Remédier à un objet S3 potentiellement malveillant](#).

Protection contre les programmes malveillants pour les types de recherche de Backup

GuardDuty Malware Protection for Backup fournit une recherche unique pour toutes les menaces détectées lors de l'analyse de la ressource demandée. Le résultat inclut le nombre total de détections effectuées pendant l'analyse et, en fonction de leur gravité, fournit des détails sur les 32 principales menaces détectées. Contrairement à d'autres GuardDuty résultats, les résultats de Malware Protection for Backup ne sont pas mis à jour lorsque la même ressource est à nouveau analysée. Une nouvelle détection de Malware Protection for Backup est générée pour chaque analyse qui détecte un logiciel malveillant.

Les résultats suivants sont spécifiques à GuardDuty Malware Protection for Backup.

Rubriques

- [Execution:EC2/MaliciousFile!Snapshot](#)
- [Execution:EC2/MaliciousFile!AMI](#)
- [Execution:EC2/MaliciousFile!RecoveryPoint](#)
- [Execution:S3/MaliciousFile!RecoveryPoint](#)

Execution:EC2/MaliciousFile!Snapshot

Un fichier malveillant a été détecté dans un instantané EBS.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants pour la sauvegarde

Ce résultat indique qu'un scan GuardDuty Malware Protection for Backup a détecté un ou plusieurs fichiers malveillants dans un instantané EBS de votre environnement. Pour plus d'informations, consultez la section Menaces détectées dans le panneau de détails du résultat.

Recommandations de correction :

Si ceci est imprévu, il se peut que votre instantané soit compromis. Pour de plus amples informations, veuillez consulter [Remédier à un instantané EBS potentiellement compromis](#).

Execution:EC2/MaliciousFile!AMI

Un fichier malveillant a été détecté dans une AMI EC2.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants pour la sauvegarde

Ce résultat indique qu'un scan GuardDuty Malware Protection for Backup a détecté un ou plusieurs fichiers malveillants dans une AMI de votre environnement. Pour plus d'informations, consultez la section Menaces détectées dans le panneau de détails du résultat.

Recommandations de correction :

Si ceci est imprévu, il se peut que votre AMI soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une AMI EC2 potentiellement compromise](#).

Execution:EC2/MaliciousFile!RecoveryPoint

Un fichier malveillant a été détecté dans un point AWS de restauration Backup EC2.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants pour la sauvegarde

Ce résultat indique qu'un scan GuardDuty Malware Protection for Backup a détecté un ou plusieurs fichiers malveillants dans un point de restauration EC2 de votre environnement. Le point de récupération affecté peut être un instantané EBS ou une AMI EC2. Pour plus d'informations, consultez la section Menaces détectées dans le panneau de détails du résultat.

Recommandations de correction :

Si ceci est imprévu, il se peut que votre point de récupération EC2 soit compromis. Pour de plus amples informations, veuillez consulter [Remédier à un point de restauration EC2 potentiellement compromis](#).

Execution:S3/MaliciousFile!RecoveryPoint

Un fichier malveillant a été détecté dans un AWS Backup S3 Recovery Point.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants pour la sauvegarde

Ce résultat indique qu'un scan GuardDuty Malware Protection for Backup a détecté un ou plusieurs objets malveillants dans un point de restauration S3 de votre environnement. Pour plus d'informations, consultez la section Menaces détectées dans le panneau de détails du résultat.

Recommandations de correction :

Si ceci est imprévu, il se peut que votre point de récupération S3 soit compromis. Pour de plus amples informations, veuillez consulter [Remédier à un point de restauration S3 potentiellement compromis](#).

GuardDuty Types de recherche de protection RDS

GuardDuty RDS Protection détecte un comportement de connexion anormal sur votre instance de base de données. Les résultats suivants sont spécifiques au [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et comporteront un type de ressource RDSDBInstance ou RDSLimitlessDB. La gravité et les détails des résultats diffèrent selon le type de résultat.

Rubriques

- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.FailedLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce](#)
- [CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/MaliciousIPCaller.FailedLogin](#)
- [Discovery:RDS/MaliciousIPCaller](#)

- [CredentialAccess:RDS/TorIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/TorIPCaller.FailedLogin](#)
- [Discovery:RDS/TorIPCaller](#)
- [Exfiltration:RDS/AnomalousBehavior](#)
- [Impact:RDS/AnomalousBehavior.Drop](#)
- [Impact:RDS/AnomalousBehavior.Delete](#)
- [Exfiltration:RDS/MaliciousIPCaller](#)
- [Exfiltration:RDS/TorIPCaller](#)
- [Impact:RDS/MaliciousIPCaller](#)
- [Impact:RDS/TorIPCaller](#)

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte de manière anormale.

Gravité par défaut : variable

Note

Selon le comportement anormal associé à ce résultat, la gravité par défaut peut être Faible, Moyenne ou Élevée.

- Faible : si le nom d'utilisateur associé à ce résultat s'est connecté à partir d'une adresse IP associée à un réseau privé.
- Moyenne : si le nom d'utilisateur associé à ce résultat s'est connecté à partir d'une adresse IP publique.
- Élevée : s'il existe un modèle constant de tentatives de connexion infructueuses à partir d'adresses IP publiques indiquant des stratégies d'accès trop permissives.

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous indique qu'une connexion réussie anormale a été observée sur une base de données RDS de votre AWS environnement. Cela peut indiquer qu'un utilisateur inconnu s'est

connecté à une base de données RDS pour la première fois. Un scénario courant est celui d'un utilisateur interne se connectant à une base de données à laquelle des applications accèdent par programmation et non des utilisateurs individuels.

Cette connexion réussie a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle de ML évalue tous les événements de connexion à la base de données dans votre [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de l'activité de connexion RDS, tels que l'utilisateur qui a fait la demande, l'emplacement d'origine la demande et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur les événements de connexion potentiellement inhabituels, veuillez consulter [Anomalies basées sur l'activité de connexion RDS](#).

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour détecter les activités effectuées par l'utilisateur anormal. Les résultats de gravité moyenne ou élevée peuvent indiquer que la stratégie d'accès à la base de données est trop permissive et que les informations d'identification des utilisateurs ont peut-être été divulguées ou compromises. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion réussie](#).

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Une ou plusieurs tentatives de connexion infructueuses inhabituelles ont été observées sur une base de données RDS de votre compte.

Gravité par défaut : faible

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous indique qu'un ou plusieurs échecs de connexion anormaux ont été observés sur une base de données RDS de votre environnement. AWS L'échec des tentatives de connexion à partir d'adresses IP publiques peut indiquer que la base de données RDS de votre compte a fait l'objet d'une tentative d'attaque par force brute par un acteur potentiellement malveillant.

Ces échecs de connexion ont été identifiés comme anormaux par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle de ML évalue tous les événements de connexion à la base de données dans votre [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de l'activité de connexion RDS, tels que l'utilisateur qui a fait la demande, l'emplacement d'origine la demande et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur les activités de connexion RDS potentiellement inhabituelles, veuillez consulter [Anomalies basées sur l'activité de connexion RDS](#).

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la base de données est exposée au public ou que la stratégie d'accès à la base de données est trop permissive. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion échouée](#).

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte à partir d'une adresse IP publique de manière anormale en suivant un modèle constant de tentatives de connexion infructueuses inhabituelles.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous indique qu'une connexion anormale indiquant une force brute réussie a été observée sur une base de données RDS de votre AWS environnement. Avant une connexion réussie anormale, un modèle constant de tentatives de connexion infructueuses inhabituelles a été observé. Cela indique que l'utilisateur et le mot de passe associés à la base de données RDS dans votre compte ont peut-être été compromis et qu'un acteur potentiellement malveillant a peut-être accédé à la base de données RDS.

Cette connexion par force brute réussie a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) par détection d' GuardDuty anomalies. Le modèle de ML évalue

tous les événements de connexion à la base de données dans votre [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de l'activité de connexion RDS, tels que l'utilisateur qui a fait la demande, l'emplacement d'origine la demande et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur les activités de connexion RDS potentiellement inhabituelles, veuillez consulter [Anomalies basées sur l'activité de connexion RDS](#).

Recommandations de correction :

Cette activité indique que les informations d'identification de la base de données ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour prendre connaissance des activités effectuées par l'utilisateur potentiellement compromis. Un modèle constant de tentatives de connexion infructueuses inhabituelles indique une stratégie d'accès à la base de données trop permissive ou que la base de données peut également avoir été exposée publiquement. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion réussie](#).

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous indique qu'une activité de connexion RDS réussie s'est produite à partir d'une adresse IP associée à une activité malveillante connue dans votre AWS environnement. Cela indique que l'utilisateur et le mot de passe associés à la base de données RDS dans votre compte ont peut-être été compromis et qu'un acteur potentiellement malveillant a peut-être accédé à la base de données RDS.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour prendre connaissance des activités effectuées par l'utilisateur compromis. Cette activité peut également indiquer qu'il existe une stratégie d'accès trop permissive à la base de données ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion réussie](#).

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Une adresse IP associée à une activité malveillante connue a tenté en vain de se connecter à une base de données RDS dans votre compte.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous indique qu'une adresse IP associée à une activité malveillante connue a tenté de se connecter à une base de données RDS dans votre AWS environnement, mais n'a pas fourni le nom d'utilisateur ou le mot de passe correct. Cela indique qu'un acteur potentiellement malveillant tente peut-être de compromettre la base de données RDS dans votre compte.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion échouée](#).

Discovery:RDS/MaliciousIPCaller

Une adresse IP associée à une activité malveillante connue a effectué une recherche dans une base de données RDS de votre compte. Aucune tentative d'authentification n'a été effectuée.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous indique qu'une adresse IP associée à une activité malveillante connue a sondé une base de données RDS dans votre AWS environnement, bien qu'aucune tentative de connexion n'ait été effectuée. Cela peut indiquer qu'un acteur potentiellement malveillant tente de rechercher une infrastructure accessible au public.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion échouée](#).

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte à partir d'une adresse IP du nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'un utilisateur est parvenu à se connecter à une base de données RDS de votre environnement AWS , à partir d'une adresse IP du nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud

Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé aux ressources RDS dans votre compte, dans le but de masquer la véritable identité de l'utilisateur anonyme.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour prendre connaissance des activités effectuées par l'utilisateur compromis. Cette activité peut également indiquer qu'il existe une stratégie d'accès trop permissive à la base de données ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion réussie](#).

CredentialAccess:RDS/TorIPCaller.FailedLogin

Une adresse IP Tor a tenté de se connecter sans succès à une base de données RDS dans votre compte.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Cette découverte vous indique qu'une adresse IP du nœud de sortie Tor a tenté de se connecter à une base de données RDS dans votre AWS environnement, mais n'a pas fourni le nom d'utilisateur ou le mot de passe correct. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé aux ressources RDS dans votre compte, dans le but de masquer la véritable identité de l'utilisateur anonyme.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du

groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion échouée](#).

Discovery:RDS/TorIPCaller

Une adresse IP du nœud de sortie Tor a effectué une recherche dans une base de données RDS de votre compte, aucune tentative d'authentification n'a eu lieu.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une adresse IP du nœud de sortie Tor a effectué une recherche dans une base de données RDS dans votre environnement AWS , bien qu'aucune tentative de connexion n'ait eu lieu. Cela peut indiquer qu'un acteur potentiellement malveillant tente de rechercher une infrastructure accessible au public. Tor est un logiciel permettant d'activer les communications anonymes. Il chiffre et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé aux ressources RDS dans votre compte, dans le but de masquer la véritable identité de l'acteur potentiellement malveillant.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Correction d'une base de données potentiellement compromise avec des événements de connexion échouée](#).

Exfiltration:RDS/AnomalousBehavior

Activité anormale d'un utilisateur extrayant un volume important de données d'une base de données RDS de votre compte.

Gravité par défaut : faible

 Note

Selon le comportement anormal associé à ce résultat, la gravité par défaut peut être faible, moyenne ou élevée.

- Faible — Si le nom d'utilisateur associé à cette recherche a exécuté SELECT des instructions à partir d'une adresse IP associée à un réseau privé.
- Moyen — Si le nom d'utilisateur associé à cette découverte a exécuté SELECT des instructions à partir d'une adresse IP publique.
- Élevé : si le nom d'utilisateur associé à ce résultat a exécuté SELECT des instructions renvoyant un volume de lignes anormalement important et que l'activité provenait d'un réseau public invisible auparavant ou était exécutée par un rôle de base de données ou un client administratif à privilèges élevés.

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Ce résultat vous indique qu'une activité de base de données anormale correspondant à une exfiltration de données a été observée sur une base de données RDS de votre environnement. AWS Cela peut indiquer qu'un utilisateur de base de données a sélectionné un nombre de lignes nettement plus élevé que d'habitude, ou que l'activité impliquait un attribut de base de données invisible, tel qu'un nouvel utilisateur, une adresse IP ou un nouveau nom de base de données, qui a contribué au pic de volume. Un scénario courant est celui d'un identifiant de base de données compromis utilisé pour extraire des données en combinant des modèles d'accès inhabituels et un volume de requêtes élevé.

Cette activité a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle ML évalue tous les événements liés à l'activité de votre base de données [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit différents facteurs de l'activité de la base de données RDS, tels que l'utilisateur qui a fait la demande, les requêtes exécutées, le volume de données consultées et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur l'activité de base de données potentiellement inhabituelle, consultez [Anomalies liées à l'activité des données RDS](#).

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour déterminer les données auxquelles l'utilisateur anormal a accédé. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité d'exfiltration anormale](#).

Impact:RDS/AnomalousBehavior.Drop

Activité anormale due à la suppression par un utilisateur de données d'une base de données RDS dans votre compte.

Gravité par défaut : moyenne

Note

Selon le comportement anormal associé à ce résultat, la gravité par défaut peut être moyenne ou élevée.

- Moyen — Si le nom d'utilisateur associé à cette constatation exécutait des DROP instructions anormales.
- Élevé : si le nom d'utilisateur associé à cette constatation a exécuté plusieurs DROP instructions et que l'activité provient d'un réseau public invisible auparavant ou a été exécutée par un rôle de base de données ou un client administratif à privilèges élevés.

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Ce résultat vous indique qu'une activité de base de données anormale correspondant à des opérations destructrices a été observée sur une base de données RDS de votre AWS environnement. Cela peut indiquer qu'un utilisateur de base de données a supprimé un nombre nettement plus élevé de tables ou d'objets de base de données que d'habitude, ou que l'activité impliquait un attribut de base de données invisible, tel qu'un nouvel utilisateur, une nouvelle adresse IP ou un nouveau nom d'application, qui a contribué à l'opération destructrice. Un scénario courant est celui d'un identifiant de base de données compromis utilisé pour détruire des structures de base de données en combinant des modèles d'accès inhabituels et un volume d'DROP instructions élevé.

Cette activité a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle ML évalue tous les événements liés à l'activité de votre base de données [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit différents facteurs de l'activité de la base de données RDS, tels que l'utilisateur qui a fait la demande, les instructions exécutées, les objets de base de données ciblés et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur l'activité de base de données potentiellement inhabituelle, consultez [Anomalies liées à l'activité des données RDS](#).

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, il est recommandé de modifier immédiatement le mot de passe de l'utilisateur de base de données associé et de révoquer son accès. Passez en revue les journaux d'audit disponibles pour déterminer l'étendue des objets supprimés et lancez la restauration à partir des sauvegardes si nécessaire. Il est également recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité destructrice anormale](#).

Impact:RDS/AnomalousBehavior.Delete

Activité anormale de la part d'un utilisateur qui supprime des données d'une base de données RDS de votre compte.

Gravité par défaut : faible

Note

Selon le comportement anormal associé à ce résultat, la gravité par défaut peut être faible, moyenne ou élevée.

- Faible — Si le nom d'utilisateur associé à cette recherche a exécuté DELETE des instructions à partir d'une adresse IP associée à un réseau privé.
- Moyen — Si le nom d'utilisateur associé à cette découverte a exécuté DELETE des instructions à partir d'une adresse IP publique.
- Élevé : si le nom d'utilisateur associé à ce résultat a exécuté DELETE des instructions renvoyant un volume de lignes anormalement important et que l'activité provenait d'un

réseau public invisible auparavant ou était exécutée par un rôle de base de données ou un client administratif à privilèges élevés.

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Ce résultat vous indique qu'une activité de base de données anormale correspondant à des opérations destructrices a été observée sur une base de données RDS de votre AWS environnement. Cela peut indiquer qu'un utilisateur de base de données a supprimé un nombre de lignes nettement plus élevé que d'habitude, ou que l'activité impliquait un attribut de base de données invisible, tel qu'un nouvel utilisateur, une nouvelle adresse IP ou un nouveau nom d'application, qui a contribué à l'opération destructrice. Un scénario courant est celui d'un identifiant de base de données compromis utilisé pour supprimer systématiquement des données en combinant des modèles d'accès inhabituels et un volume de DELETE relevés élevé.

Cette activité a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle ML évalue tous les événements liés à l'activité de votre base de données [Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge](#) et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit différents facteurs de l'activité de la base de données RDS, tels que l'utilisateur qui a fait la demande, les instructions exécutées, le nombre de lignes affectées et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur l'activité de base de données potentiellement inhabituelle, consultez [Anomalies liées à l'activité des données RDS](#).

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, il est recommandé de modifier immédiatement le mot de passe de l'utilisateur de base de données associé et de révoquer son accès. Passez en revue les journaux d'audit disponibles pour déterminer l'étendue des données supprimées et lancez une restauration instantanée à partir de sauvegardes automatisées si la perte de données est confirmée. Il est également recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité destructrice anormale](#).

Exfiltration:RDS/MaliciousIPCaller

Une adresse IP associée à une activité malveillante connue a exécuté des requêtes d'extraction de données sur une base de données RDS de votre compte.

Gravité par défaut : élevée

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Ce résultat vous indique qu'une adresse IP associée à une activité malveillante connue a exécuté des requêtes de base de données compatibles avec l'exfiltration de données sur une base de données RDS de votre AWS environnement. Cela indique que l'utilisateur et le mot de passe associés à la base de données RDS de votre compte ont peut-être été compromis et que les données de la base de données RDS ont peut-être été exfiltrées par un acteur potentiellement malveillant.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux de données RDS disponibles pour détecter les activités effectuées par l'utilisateur compromis. Il est recommandé d'identifier les données accessibles à l'utilisateur concerné et d'évaluer l'impact commercial de toute donnée potentiellement exfiltrée. Il est également recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité d'exfiltration anormale](#).

Exfiltration:RDS/TorIPCaller

Une adresse IP du nœud de sortie Tor a exécuté des requêtes d'extraction de données sur une base de données RDS de votre compte.

Gravité par défaut : élevée

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Cette découverte vous indique qu'une adresse IP du nœud de sortie Tor a exécuté des requêtes de base de données cohérentes avec l'exfiltration de données sur une base de données RDS de votre AWS environnement. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut indiquer un accès non autorisé aux ressources RDS de votre compte, dans le but de masquer la véritable identité de l'utilisateur anonyme lors de l'exfiltration des données.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux de données RDS disponibles pour détecter les activités effectuées par l'utilisateur compromis. Il est recommandé d'identifier les données accessibles à l'utilisateur concerné et d'évaluer l'impact commercial de toute donnée potentiellement exfiltrée. Il est également recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité d'exfiltration anormale](#).

Impact:RDS/MaliciousIPCaller

Une adresse IP associée à une activité malveillante connue a exécuté des instructions destructrices sur une base de données RDS de votre compte.

Gravité par défaut : élevée

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Ce résultat vous indique qu'une adresse IP associée à une activité malveillante connue a exécuté des instructions de base de données avec un impact destructeur sur une base de données RDS de votre AWS environnement. Cela indique que l'utilisateur et le mot de passe associés à la base de données RDS de votre compte ont peut-être été compromis et que la base de données RDS a peut-être été soumise à des opérations destructrices par un acteur potentiellement malveillant.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier immédiatement le mot de passe de l'utilisateur de base de données associé et de révoquer son accès. Passez en revue les journaux de données RDS disponibles pour déterminer l'étendue des opérations destructrices effectuées, et lancez la restauration à partir des sauvegardes si nécessaire. Il est également recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité destructrice anormale](#).

Impact:RDS/TorIPCaller

Une adresse IP du nœud de sortie Tor a exécuté des instructions destructrices sur une base de données RDS de votre compte.

Gravité par défaut : élevée

- Fonctionnalité : Surveillance de l'activité de la base de données RDS

Cette découverte vous indique qu'une adresse IP du nœud de sortie Tor a exécuté des instructions de base de données avec un impact destructeur sur une base de données RDS de votre AWS environnement. Tor est un réseau superposé permettant une communication anonyme. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut indiquer un accès non autorisé aux ressources RDS de votre compte, dans le but de masquer la véritable identité de l'utilisateur anonyme tout en effectuant des opérations destructrices.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier immédiatement le mot de passe de l'utilisateur de base de données associé et de révoquer son accès. Passez en revue les journaux de données RDS disponibles pour déterminer l'étendue des opérations destructrices effectuées, et lancez la restauration à partir des sauvegardes si nécessaire. Il est également recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Corriger une base de données potentiellement compromise par une activité destructrice anormale](#).

Types de résultat de la protection Lambda

Cette section décrit les types de recherche spécifiques à vos AWS Lambda ressources et resourceType répertoriés commeLambda. Pour tous les résultats Lambda, nous vous recommandons d'examiner la ressource en question et de déterminer si elle se comporte comme prévu. Si l'activité est autorisée, vous pouvez utiliser des [règles de suppression](#) ou des [adresses IP approuvées et des listes de menaces](#) pour éviter les notifications faussement positives pour cette ressource.

Si l'activité est inattendue, la bonne pratique en matière de sécurité consiste à partir du principe que Lambda a été potentiellement compromis et à suivre les recommandations de correction.

Rubriques

- [Backdoor:Lambda/C&CActivity.B](#)
- [CryptoCurrency:Lambda/BitcoinTool.B](#)
- [Trojan:Lambda/BlackholeTraffic](#)
- [Trojan:Lambda/DropPoint](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:Lambda/TorClient](#)
- [UnauthorizedAccess:Lambda/TorRelay](#)

Backdoor:Lambda/C&CActivity.B

Une fonction Lambda interroge une adresse IP associée à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous indique qu'une fonction Lambda répertoriée dans votre AWS environnement interroge une adresse IP associée à un serveur de commande et de contrôle (C&C) connu. La fonction Lambda associée au résultat généré est potentiellement compromise. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui est infecté et contrôlé par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer un déni de service distribué (DDoS).

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

CryptoCurrency:Lambda/BitcoinTool.B

Une fonction Lambda interroge une adresse IP associée à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous indique que la fonction Lambda répertoriée dans votre AWS environnement interroge une adresse IP associée à un Bitcoin ou à une autre activité liée aux cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des fonctions Lambda afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

Recommandations de correction :

Si vous utilisez cette fonction Lambda pour exploiter ou gérer des cryptomonnaies, ou si cette fonction est impliquée d'une autre manière dans une activité de blockchain, il s'agit potentiellement d'une activité attendue pour votre environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur CryptoCurrency:Lambda/BitcoinTool.B. Le deuxième critère de filtre doit être le nom de la fonction Lambda de la fonction impliquée dans l'activité de blockchain. Pour plus d'informations sur la création de règles de suppression, consultez [Règles de suppression](#).

Si cette activité est imprévue, il est possible que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

Trojan:Lambda/BlackholeTraffic

Une fonction Lambda tente de communiquer avec une adresse IP d'un hôte distant qui est un trou noir connu.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous indique qu'une fonction Lambda répertoriée dans votre AWS environnement essaie de communiquer avec l'adresse IP d'un trou noir (ou d'un puits). Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire. Une adresse IP de trou noir désigne une machine hôte qui n'est pas en cours d'exécution ou une adresse à laquelle aucun hôte n'a été attribué. La fonction Lambda répertoriée est potentiellement compromise.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

Trojan:Lambda/DropPoint

Une fonction Lambda tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous indique qu'une fonction Lambda répertoriée dans votre AWS environnement essaie de communiquer avec l'adresse IP d'un hôte distant connu pour détenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Une fonction Lambda établit des connexions à une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous indique qu'une fonction Lambda de votre AWS environnement communique avec une adresse IP figurant sur une liste de menaces que vous avez téléchargée. Dans GuardDuty, une [liste de menaces](#) est composée d'adresses IP malveillantes connues. GuardDuty génère des résultats sur la base des listes de menaces téléchargées. Vous pouvez consulter les détails de la liste des menaces dans les informations de recherche de la GuardDuty console.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

UnauthorizedAccess:Lambda/TorClient

Une fonction Lambda est en train de se connecter à un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Cette découverte vous indique qu'une fonction Lambda de votre AWS environnement établit des connexions à un nœud Tor Guard ou Authority. Tor est un logiciel permettant d'activer les communications anonymes. Le nœud Tor Guard et Authority agit en tant que passerelles initiales dans un réseau Tor. Ce trafic peut indiquer que cette fonction Lambda a été potentiellement compromise. Il agit désormais en tant que client sur un réseau Tor.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

UnauthorizedAccess:Lambda/TorRelay

Une fonction Lambda est en train de se connecter à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Cette découverte vous indique qu'une fonction Lambda de votre AWS environnement établit des connexions à un réseau Tor d'une manière qui suggère qu'elle agit comme un relais Tor. Tor est un logiciel permettant d'activer les communications anonymes. Tor active une communication anonyme en réacheminant le trafic potentiellement illicite du client d'un relais Tor à un autre.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter [Corriger une fonction Lambda potentiellement compromise](#).

GuardDuty Types de détection de protection contre l'IA

Lorsque vous activez AI Protection, GuardDuty analyse les événements de AWS CloudTrail gestion et les événements de données provenant d'Amazon Bedrock et d'Amazon SageMaker AI. GuardDuty utilise ces données pour détecter les activités potentiellement suspectes qui ciblent vos charges de travail d'IA. Lorsqu'il GuardDuty détecte une menace potentielle, il génère l'un des types de détection suivants. La `Resource` type raison de ces résultats est `AccessKey`, et la découverte identifie l'identité IAM qui a invoqué le modèle.

Chaque découverte inclut également des détails sur les ressources d'IA affectées dans l'objet de la découverte. [Impact:IAMUser/CostHarvesting](#) Les résultats incluent une `resource.modelDetails` liste qui identifie les modèles Amazon Bedrock ou Amazon SageMaker AI invoqués. [Impact:IAMUser/AnomalousModelInvocation](#) La [Impact:IAMUser/PromptInjection.Direct](#) découverte inclut un `resource.bedrockGuardrailDetails` objet qui décrit le garde-corps Amazon Bedrock qui est intervenu. Vous pouvez consulter ces informations dans la GuardDuty console ou dans le JSON de recherche.

Les types de [Impact:IAMUser/CostHarvesting](#) recherche [Impact:IAMUser/AnomalousModelInvocation](#) et s'appliquent à la fois aux invocations de modèles Amazon Bedrock et Amazon SageMaker AI. Le

type de [Impact:IAMUser/PromptInjection.Direct](#) recherche s'applique aux charges de travail Amazon Bedrock qui utilisent Amazon Bedrock Guardrails.

Rubriques

- [Impact:IAMUser/AnomalousModelInvocation](#)
- [Impact:IAMUser/CostHarvesting](#)
- [Impact:IAMUser/PromptInjection.Direct](#)

Impact:IAMUser/AnomalousModelInvocation

Une identité IAM a invoqué un modèle Amazon Bedrock ou Amazon SageMaker AI d'une manière différente de la référence établie pour l'identité ou le compte.

Gravité par défaut : faible

- Fonctionnalité : Protection contre l'IA

Cette découverte vous indique qu'une identité IAM a invoqué un modèle Amazon Bedrock ou Amazon SageMaker AI d'une manière différente de l'activité historique de l'identité ou du compte. Cette activité peut indiquer qu'un acteur malveillant utilise des informations d'identification compromises pour accéder aux modèles de base de votre compte. Par exemple, l'acteur peut sonder un modèle, créer des entrées contradictoires ou exécuter des requêtes automatisées.

GuardDuty établit une base de référence pour l'activité d'invocation normale des modèles pour chaque identité IAM et Compte AWS qui invoque Amazon Bedrock ou Amazon AI. SageMaker GuardDuty présente les caractéristiques de l'activité d'invocation, notamment les suivantes :

- L'API d'invocation du modèle que l'identité a appelée
- Le modèle invoqué par l'identité
- L'adresse IP source et son organisation ASN (Autonomous System Number) associée
- L'agent utilisateur qui a effectué la demande

Lorsqu'une GuardDuty activité observée s'écarte de manière significative de cette base de référence, elle génère ce résultat. Les exemples incluent les appels à partir d'une adresse IP inédite, d'un agent utilisateur invisible ou d'un modèle que l'identité n'a jamais invoqué. La découverte comprend une ressource `modelDetails` liste identifiant les modèles impliqués dans l'activité suspecte. Chaque

entrée contient un `modelId` modèle de base Amazon Bedrock, un profil d'inférence, un ARN de modèle provisionné, personnalisé ou importé, un point de terminaison Amazon Bedrock Marketplace, une ressource rapide ou le nom du point de terminaison Amazon SageMaker AI.

Cette découverte correspond à la technique [MITRE ATLAS AML.T0040 - Accès à l'API d'inférence de modèles d'IA](#) sur le site Web de MITRE ATLAS.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Pour réduire le risque d'invocations de modèles non autorisées, limitez les identités qui peuvent invoquer des modèles. Étendez l'accès aux API d'appel de modèles suivantes uniquement aux principaux et aux modèles qui en ont besoin :

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Pour empêcher l'inférence de modèles dans votre organisation lorsqu'elle n'est pas nécessaire, vous pouvez utiliser une politique de contrôle des services (SCP). Pour plus d'informations, consultez des exemples de [Identity-based politiques pour Amazon Bedrock](#) dans le guide de l'utilisateur Amazon Bedrock et des exemples de politiques basées sur l'identité [Amazon SageMaker AI](#) dans le guide du développeur Amazon SageMaker AI.

Impact: IAMUser/CostHarvesting

Une identité IAM a invoqué un modèle Amazon Bedrock ou Amazon SageMaker AI avec des volumes de jetons anormaux susceptibles d'indiquer une attaque de collecte de coûts.

Gravité par défaut : faible

- Fonctionnalité : Protection contre l'IA

Cette découverte vous indique qu'une identité IAM a invoqué un modèle Amazon Bedrock ou Amazon SageMaker AI avec des volumes de jetons d'entrée ou de sortie qui s'écartent considérablement de la base de référence pour l'identité ou le compte. Lors d'une attaque de collecte des coûts, un acteur malveillant envoie des entrées coûteuses en matière de calcul à un modèle afin d'augmenter les coûts d'exploitation de la charge de travail liée à l'IA, sans nécessairement exfiltrer les données. Ces entrées peuvent comprendre des invites trop longues ou délibérément mal formées.

GuardDuty établit une base de référence pour le volume moyen de jetons d'entrée et le volume moyen de jetons de sortie pour chaque identité et chaque compte IAM qui invoquent les modèles Amazon Bedrock ou Amazon SageMaker AI. Lorsque GuardDuty observe des appels dont le nombre de jetons dépasse cette ligne de base et met en corrélation l'anomalie de volume avec d'autres signaux inhabituels, GuardDuty génère ce résultat. La découverte indique l'activité anormale de `service.detectionobjet`, y compris l'invocation observée et les volumes de jetons qui s'écartaient de la ligne de base. Il comprend également une `resource.modelDetails` liste identifiant les modèles ciblés. Chaque entrée contient un `modelId` modèle de base Amazon Bedrock, un profil d'inférence, un ARN de modèle provisionné, personnalisé ou importé, un point de terminaison Amazon Bedrock Marketplace, une ressource rapide ou le nom du point de terminaison Amazon SageMaker AI.

Cette découverte correspond à la technique [MITRE ATLAS AML.T0034 - Cost Harvesting](#) sur le site Web de MITRE ATLAS.

Recommandations de correction :

Si cette activité est inattendue pour l'identité associée, les informations d'identification ont peut-être été compromises et utilisées pour augmenter le coût de vos charges de travail d'IA. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS](#)

[informations d'identification](#). Passez en revue les appels de modèles associés à l'identité et limitez l'accès aux modèles concernés en limitant l'accès aux API d'appel de modèles suivantes aux seuls mandants qui en ont besoin :

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Pour détecter et contenir les dépenses anormales, vous pouvez utiliser [AWS les budgets](#), y compris les actions budgétaires qui appliquent une politique IAM restrictive lorsqu'un seuil budgétaire est dépassé, et la détection des anomalies de [AWS coûts](#). Pour attribuer les coûts Amazon Bedrock à des charges de travail spécifiques, vous pouvez associer des balises de répartition des coûts à un profil d'inférence d'[application](#).

Impact:IAMUser/PromptInjection.Direct

Une barrière de protection Amazon Bedrock a détecté une tentative d'injection d'invite directe lors d'une invocation effectuée par une identité IAM.

Gravité par défaut : faible

- Fonctionnalité : Protection contre l'IA

Ce résultat vous indique qu'une barrière de protection Amazon Bedrock configurée pour une charge de travail Amazon Bedrock sur votre compte a détecté une tentative d'injection d'invite directe. Dans le cadre d'une attaque par injection directe, un acteur de la menace crée une invite malveillante en tant qu'entrée dans un modèle de base. L'invite oblige le modèle à ignorer ses instructions d'origine et à suivre les instructions de l'attaquant à la place. L'injection d'invite peut donner à un attaquant un accès initial lui permettant de prendre des mesures supplémentaires contre une application d'IA, comme l'exfiltration de données, l'appel à des outils non autorisés ou le contournement des contrôles de sécurité.

GuardDuty génère ce résultat lorsqu'un Amazon Bedrock Guardrail intervient lors d'une invocation car il a détecté une attaque rapide avec un niveau de confiance élevé. GuardDuty Pour permettre de détecter l'injection directe et rapide, configurez un Amazon Bedrock Guardrail avec un filtre de contenu d'attaque [rapide](#). Pour vous assurer que le garde-fou évalue les appels dans votre environnement, appliquez-le de manière générale au lieu de vous fier à des applications individuelles pour les joindre à chaque demande. Vous pouvez appliquer une protection pour toutes les invocations du modèle Amazon Bedrock dans un compte ou au sein de votre organisation en utilisant les politiques Amazon Bedrock dans AWS Organizations Pour plus d'informations, consultez la section [Appliquer des mesures de protection entre comptes dans le cadre des mesures d'application d'Amazon Bedrock Guardrails](#) dans le guide de l'utilisateur d'Amazon Bedrock. Lorsqu'un garde-corps évalue une invocation, Amazon Bedrock enregistre l'évaluation dans des événements de AWS CloudTrail données, qui les GuardDuty analyse pour générer ce résultat. Si le garde-fou a également appliqué un filtre d'informations [sensibles](#) lors de l'évaluation de l'invocation, le résultat inclut des détails sur le type d'informations sensibles détectées.

Le résultat comprend un objet `resource.bedrockGuardrailDetails` qui décrit la barrière de protection qui est intervenue. Le tableau suivant décrit les champs de cet objet.

Champ	Description
<code>guardrails</code>	Une liste des garde-corps qui ont évalué l'invocation. Chaque entrée inclut le nom de la ressource Amazon (arn) et le nom <code>version</code> du garde-corps. Plusieurs garde-corps peuvent apparaître lorsqu'un garde-corps appliqué par le compte ou par l'organisation et un garde-corps au niveau de la demande évaluent la même invocation.
<code>guardrailAction</code>	L'action entreprise par le garde-corps. GuardDuty génère ce résultat lorsque la valeur est <code>GUARDRAIL_INTERVENED</code> .
<code>guardrailSource</code>	Le contenu évalué par le garde-corps. <code>INPUT</code> indique une invite envoyée au modèle et <code>OUTPUT</code> indique une réponse du modèle.
<code>contentPolicyFilters</code>	Liste des filtres de politique de contenu appliqués par le garde-fou. Pour ce type de recherche, une entrée comporte un type de <code>PROMPT_ATTACK</code> et un <code>confidence</code> de <code>HIGH</code> . <code>action</code> C'est <code>BLOCKED</code> si le garde-corps a bloqué le contenu ou <code>NONE</code> si le garde-corps a détecté l'attaque rapide mais a été configuré uniquement pour la signaler.

Champ	Description
<code>sensitiveInformationFilters</code>	Filtres d'informations sensibles que le garde-fou a appliqués lors de l'évaluation de l'invocation. Chaque entrée comporte un identifiant type identifiant le type d'informations sensibles détectées par le garde-corps, par exemple <code>AWS_SECRET_KEY</code> ou <code>PASSWORD</code> , et indiquant si le garde-corps a bloqué le contenu, <code>BLOCKED</code> si le garde-corps l'a masqué ou <code>ANONYMIZED</code> <code>NONE</code> si le garde-corps l'a détecté mais a été configuré uniquement pour le signaler. <code>action</code> La découverte enregistre le type d'informations détectées, jamais le contenu lui-même.

Cette découverte correspond à la technique [MITRE ATLAS AML.T0051 - LLM Prompt Injection](#) sur le site Web de MITRE ATLAS.

Recommandations de correction :

Vérifiez l'invite qui a déclenché l'intervention de la barrière de sécurité et l'identité IAM qui a envoyé l'invite. Si l'activité est inattendue pour l'identité associée, les informations d'identification ont peut-être été compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#). Si le garde-corps a détecté l'attaque rapide mais ne l'a pas bloquée, envisagez de définir l'action du filtre de contenu d'attaque rapide sur `Bloquer` plutôt que sur `Détecter` afin que le garde-corps bloque le contenu. Pour plus d'informations, consultez la section [Options de gestion du contenu préjudiciable détecté par Amazon Bedrock Guardrails](#) dans le guide de l'utilisateur d'Amazon Bedrock. Vous pouvez également restreindre l'accès aux API d'appel Amazon Bedrock pour l'identité concernée.

Retrait de types de résultat

Un résultat est une notification qui contient des détails sur un problème de sécurité potentiel découvert par GuardDuty . Pour plus d'informations sur les modifications importantes apportées aux types de GuardDuty recherche, y compris les types de recherche récemment ajoutés ou retirés, voir [Historique du document pour Amazon GuardDuty](#).

Les types de recherche suivants sont retirés et ne sont plus générés par GuardDuty.

⚠ Important

Vous ne pouvez pas réactiver les types de GuardDuty recherche retirés.

Rubriques

- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Exfiltration:S3/ObjectRead.Unusual](#)
- [Impact:S3/PermissionsModification.Unusual](#)
- [Impact:S3/ObjectDelete.Unusual](#)
- [Discovery:S3/BucketEnumeration.Unusual](#)
- [Persistence:IAMUser/NetworkPermissions](#)
- [Persistence:IAMUser/ResourcePermissions](#)
- [Persistence:IAMUser/UserPermissions](#)
- [PrivilegeEscalation:IAMUser/AdministrativePermissions](#)
- [Recon:IAMUser/NetworkPermissions](#)
- [Recon:IAMUser/ResourcePermissions](#)
- [Recon:IAMUser/UserPermissions](#)
- [ResourceConsumption:IAMUser/ComputeResources](#)
- [Stealth:IAMUser/LoggingConfigurationModified](#)
- [UnauthorizedAccess:IAMUser/ConsoleLogin](#)
- [UnauthorizedAccess:EC2/TorIPCaller](#)
- [Backdoor:EC2/XORDDOS](#)
- [Behavior:IAMUser/InstanceLaunchUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.A](#)
- [UnauthorizedAccess:IAMUser/UnusualASNCaller](#)

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Un conteneur privilégié avec accès au niveau racine a été lancé sur votre cluster Kubernetes.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'un conteneur privilégié a été lancé sur votre cluster Kubernetes à l'aide d'une image qui n'a jamais été utilisée auparavant pour lancer des conteneurs privilégiés dans votre cluster. Un conteneur privilégié dispose d'un accès au niveau racine à l'hôte. Les adversaires peuvent lancer des conteneurs privilégiés comme tactique d'escalade des privilèges pour accéder à l'hôte puis le compromettre.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent être compromises. Révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Persistence:Kubernetes/ContainerWithSensitiveMount

Un conteneur a été lancé avec un chemin d'accès de l'hôte externe sensible monté à l'intérieur.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'un conteneur a été lancé avec une configuration incluant un chemin d'accès de l'hôte sensible avec accès en écriture dans la section `volumeMounts`. Cela rend le chemin d'accès de l'hôte sensible accessible et inscriptible depuis l'intérieur du conteneur. Cette technique est couramment utilisée par des adversaires pour accéder au système de fichiers de l'hôte.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent être compromises. Révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter [Corriger les résultats de la protection EKS](#).

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression composée de critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit être identique au `imagePrefix` spécifié dans le résultat. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter [Règles de suppression](#) (langue française non garantie).

Exfiltration:S3/ObjectRead.Unusual

Une entité IAM a invoqué une API S3 de manière suspecte.

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous indique qu'une entité IAM de votre AWS environnement effectue des appels d'API qui impliquent un compartiment S3 et qui diffèrent de la base de référence établie pour cette entité. L'appel d'API utilisé dans cette activité est associé à la phase d'exfiltration d'une attaque, au cours de laquelle un pirate tente de collecter des données. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives.

Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Impact:S3/PermissionsModification.Unusual

Une entité IAM a invoqué une API pour modifier les autorisations sur une ou plusieurs ressources S3.

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat vous informe qu'une entité IAM effectue des appels d'API conçus pour modifier les autorisations sur un ou plusieurs compartiments ou objets de votre environnement AWS . Cette action peut être effectuée par un pirate pour permettre le partage d'informations en dehors du compte. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Impact:S3/ObjectDelete.Unusual

Une entité IAM a invoqué une API utilisée pour supprimer les données dans un compartiment S3.

Gravité par défaut : moyenne*

 Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat vous indique qu'une entité IAM spécifique de votre AWS environnement effectue des appels d'API conçus pour supprimer les données du compartiment S3 répertorié en supprimant le compartiment lui-même. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Discovery:S3/BucketEnumeration.Unusual

Une entité IAM a invoqué une API S3 utilisée pour découvrir les compartiments S3 au sein de votre réseau.

Gravité par défaut : moyenne*

 Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat vous informe qu'une entité IAM a invoqué une API S3 pour découvrir des compartiments S3 dans votre environnement, comme `ListBuckets`. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un attaquant collecte des informations pour déterminer si votre AWS environnement est vulnérable à une attaque de plus grande envergure. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette

entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter [Remédier à un compartiment S3 potentiellement compromis](#).

Persistence:IAMUser/NetworkPermissions

Une entité IAM a invoqué une API couramment utilisée pour modifier les autorisations d'accès au réseau pour les groupes de sécurité, les itinéraires et les ACL de votre AWS .

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide AWS d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat indique qu'un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur) spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsque les paramètres de configuration réseau sont modifiés dans des circonstances suspectes, par exemple lorsqu'un principal invoque l'API `CreateSecurityGroup` alors qu'il ne l'a jamais fait auparavant. Les pirates essaient souvent de modifier des groupes de sécurité, ce qui permet le trafic entrant sur les différents ports afin d'améliorer leur capacité à accéder à une instance EC2.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Persistence:IAMUser/ResourcePermissions

Un principal a invoqué une API couramment utilisée pour modifier les politiques d'accès de sécurité de diverses ressources de votre Compte AWS.

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat indique qu'un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur) spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais appelé cette API auparavant.

Cette constatation est déclenchée lorsqu'une modification est détectée dans les politiques ou les autorisations associées aux AWS ressources, par exemple lorsqu'un responsable de votre AWS environnement invoque l'PutBucketPolicyAPI sans aucun historique en la matière. Certains services, comme Amazon S3, prennent en charge les autorisations associées à des ressources et permettant à un ou plusieurs principaux d'accéder à la ressource. Avec des informations d'identification volées, des pirates peuvent modifier les stratégies associées à une ressource pour y obtenir l'accès.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Persistence:IAMUser/UserPermissions

Un directeur a invoqué une API couramment utilisée pour ajouter, modifier ou supprimer des utilisateurs, des groupes ou des politiques IAM dans votre AWS .

Gravité par défaut : moyenne*

 Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat indique qu'un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur) spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais appelé cette API auparavant.

Cette découverte est déclenchée par des modifications suspectes apportées aux autorisations relatives aux utilisateurs dans votre AWS environnement, par exemple lorsqu'un responsable de votre AWS environnement invoque l'AttachUserPolicyAPI sans aucun historique. Les pirates peuvent utiliser des informations d'identification volées pour créer des utilisateurs, ajouter des stratégies d'accès aux utilisateurs existants ou créer des clés d'accès afin de maximiser leur accès à un compte, même si leur point d'accès d'origine est fermé. Par exemple, le propriétaire du compte peut remarquer qu'un utilisateur IAM ou un mot de passe particulier a été volé et le supprimer du compte. Cependant, il est possible qu'ils ne suppriment pas d'autres utilisateurs créés par un administrateur principal créé de manière frauduleuse, laissant leur AWS compte accessible à l'attaquant.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

PrivilegeEscalation:IAMUser/AdministrativePermissions

Un principal a tenté de s'attribuer à lui-même une stratégie très permissive.

Gravité par défaut : faible*

 Note

La gravité de ce résultat est faible si la tentative d'escalade des privilèges n'a pas abouti. Elle est moyenne si la tentative d'escalade des privilèges a réussi.

Ce résultat indique qu'une entité IAM spécifique de votre AWS environnement présente un comportement qui peut être révélateur d'une attaque par augmentation de privilèges. Ce résultat est déclenché lorsqu'un utilisateur ou un rôle IAM tente de s'attribuer à lui-même une stratégie très permissive. Si l'utilisateur ou le rôle en question n'est pas censé disposer de privilèges administratifs, les informations d'identification de l'utilisateur peuvent être compromises ou les autorisations du rôle peuvent ne pas être configurées correctement.

Les pirates utiliseront des informations d'identification volées pour créer des utilisateurs, ajouter des stratégies d'accès aux utilisateurs existants ou créer des clés d'accès afin de maximiser leur accès à un compte, même si leur point d'accès d'origine est fermé. Par exemple, le propriétaire du compte peut remarquer que les informations d'identification de connexion d'un utilisateur IAM spécifique ont été volées et les supprimer du compte, mais ne pas supprimer d'autres utilisateurs qui ont été créés par le principal administrateur frauduleusement créé, laissant leur compte AWS toujours accessible au pirate.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Recon:IAMUser/NetworkPermissions

Un principal a invoqué une API couramment utilisée pour modifier les autorisations d'accès au réseau pour les groupes de sécurité, les itinéraires et les ACL de votre AWS .

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide AWS d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat indique qu'un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur) spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsque des autorisations d'accès à des ressources dans votre compte AWS sont examinées dans des circonstances suspectes. Par exemple, si un principal a appelé l'API `DescribeInstances` alors qu'il ne l'a jamais fait auparavant. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Recon:IAMUser/ResourcePermissions

Un principal a invoqué une API couramment utilisée pour modifier les politiques d'accès de sécurité de diverses ressources de votre AWS .

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat indique qu'un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur) spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsque des autorisations d'accès à des ressources dans votre compte AWS sont examinées dans des circonstances suspectes. Par exemple, si un principal a appelé l'API `DescribeInstances` alors qu'il ne l'a jamais fait auparavant. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Recon:IAMUser/UserPermissions

Un directeur a invoqué une API couramment utilisée pour ajouter, modifier ou supprimer des utilisateurs, des groupes ou des politiques IAM dans votre AWS .

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat est déclenché lorsque les autorisations des utilisateurs de votre AWS environnement sont vérifiées dans des circonstances suspectes. Par exemple, si un principal (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur IAM) a invoqué l'API `ListInstanceProfilesForRole` alors qu'il ne l'a jamais fait auparavant. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Ce résultat indique qu'un principe spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais appelé cette API auparavant de cette manière.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

ResourceConsumption:IAMUser/ComputeResources

Un principal a appelé une API couramment utilisée pour lancer des ressources de calcul comme des instances EC2.

Gravité par défaut : moyenne*

Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide AWS d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat est déclenché lorsque des instances EC2 dans le compte répertorié au sein de votre environnement AWS sont lancées dans des circonstances suspectes. Ce résultat indique qu'un principal spécifique de votre AWS environnement présente un comportement différent de celui de la référence établie ; par exemple, si un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur IAM) a invoqué l'RunInstancesAPI sans aucun historique de ce type. Cela peut être le signe qu'un pirate utilise des informations d'identification volées pour voler du temps de calcul (peut-être pour le minage de monnaie cryptographique ou le cassage d'un mot de passe). Cela peut également indiquer qu'un attaquant utilise une instance EC2 dans votre AWS environnement et ses informations d'identification pour conserver l'accès à votre compte.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

Stealth:IAMUser/LoggingConfigurationModified

Un directeur a invoqué une API couramment utilisée pour arrêter la CloudTrail journalisation, supprimer les journaux existants et éliminer les traces d'activité dans votre AWS .

Gravité par défaut : moyenne*

 Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide AWS d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat est déclenché lorsque la configuration de la journalisation dans le compte AWS répertorié au sein de votre environnement est modifiée dans des circonstances suspectes. Ce résultat vous indique qu'un principal spécifique de votre AWS environnement présente un comportement différent de celui de la ligne de base établie ; par exemple, si un principal (Utilisateur racine d'un compte AWS rôle IAM ou utilisateur IAM) a invoqué l'API `StopLoggingAPI` sans aucun historique de ce type. Cela peut indiquer qu'un pirate tente de recouvrir ses traces toute trace de ses activités.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:IAMUser/ConsoleLogin

Une connexion inhabituelle à la console par un principal de votre AWS le compte a été observé.

Gravité par défaut : moyenne*

 Note

La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide AWS d'informations d'identification temporaires créées sur une instance, le niveau de gravité du résultat est élevé.

Ce résultat est déclenchée lorsqu'une connexion à une console est détectée dans des circonstances suspectes. Par exemple, si un directeur qui n'a jamais agi dans ce domaine a invoqué l'API `ConsoleLogin` depuis un client jamais utilisé auparavant ou depuis un emplacement inhabituel. Cela peut indiquer que des informations d'identification volées ont été utilisées pour accéder à

vosre AWS compte, ou qu'un utilisateur valide accède au compte de manière non valide ou moins sécurisée (par exemple, pas via un VPN approuvé).

Ce résultat vous indique qu'un principe spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Ce principal n'a jamais eu d'activité de connexion à l'aide de cette application client et depuis cet emplacement spécifique auparavant.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

UnauthorizedAccess:EC2/TorIPCaller

Votre instance EC2 reçoit des connexions entrantes d'un nœud d'exit Tor.

Gravité par défaut : moyenne

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement reçoit des connexions entrantes depuis un nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cette découverte peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Backdoor:EC2/XORDDOS

Une instance EC2 tente communiquer avec une adresse IP associée au programme malveillant XOR DDos.

Gravité par défaut : élevée

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement tente de communiquer avec une adresse IP associée au malware DDoS XOR. Cette instance EC2 pourrait être compromise. XOR DDoS est un cheval de Troie qui pirate les systèmes Linux. Pour accéder au système, il lance

une attaque en force afin de découvrir le mot de passe d'accès aux services Secure Shell (SSH) sur Linux. Une fois les informations d'identification SSH obtenues et la connexion réussie, il utilise les privilèges d'utilisateur root pour exécuter un script qui télécharge et installe XOR DDoS. Ce logiciel malveillant est ensuite utilisé dans le cadre d'un botnet pour lancer des attaques par déni de service (DDoS) distribué à l'encontre d'autres cibles.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

Behavior:IAMUser/InstanceLaunchUnusual

Un utilisateur a lancé une instance EC2 d'un type inhabituel.

Gravité par défaut : élevée

Ce résultat vous indique qu'un utilisateur spécifique de votre AWS environnement présente un comportement différent de celui de référence établi. Cet utilisateur n'a jamais lancé d'instances EC2 de ce type auparavant. Vos informations d'identification de connexion pourraient être compromises.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

CryptoCurrency:EC2/BitcoinTool.A

Une instance EC2 communique avec des groupes de minage de bitcoins.

Gravité par défaut : élevée

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement communique avec des pools de minage de bitcoins. Dans le domaine du minage de monnaies cryptographiques, un groupe de minage désigné le regroupement des ressources des mineurs, qui partagent leur puissance de traitement sur un réseau pour répartir les gains en fonction de leur contribution à la résolution d'un bloc. A moins que vous ne l'utilisiez à des fins de minage de bitcoins, votre instance EC2 pourrait être compromise.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

UnauthorizedAccess:IAMUser/UnusualASNCaller

Une API a été invoquée depuis une adresse IP d'un réseau inhabituel.

Gravité par défaut : élevée

Ce résultat vous indique que certaines activités ont été invoquées à partir de l'adresse IP d'un réseau inhabituel. Ce réseau n'a jamais été observé dans l'historique d'utilisation d' AWS de l'utilisateur spécifié. Cette activité peut inclure une connexion à la console, ou une tentative de lancement d'une instance EC2, de création d'un utilisateur IAM ou de modification de vos privilèges AWS , etc. Cela peut indiquer un accès non autorisé à vos AWS ressources.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).

GuardDuty recherche de types en fonction des ressources potentiellement affectées

Les pages suivantes sont classées en fonction du type de ressource potentiellement affectée associé à une GuardDuty découverte :

- [Types de résultat EC2](#)
- [Types de résultat IAM](#)
- [Types de détection de séquences d'attaques](#)
- [Règles de détection personnalisées : types de recherche](#)
- [Types de détection de la protection S3](#)
- [Types de recherche de protection EKS](#)
- [Types de recherche liés à la surveillance du temps](#)
- [Protection contre les programmes malveillants pour les types de détection EC2](#)
- [Protection contre les programmes malveillants pour le type de recherche S3](#)
- [Protection contre les programmes malveillants pour les types de recherche de Backup](#)

- [Types de résultat de la protection RDS](#)
- [Types de résultat de la protection Lambda](#)
- [Types de détection de protection contre l'IA](#)

GuardDuty types de recherche actifs

Le tableau suivant présente tous les types de détection actifs, regroupés par source : d'abord les types de découverte issus de la détection des menaces fondamentales (triés par source de données), puis les types de recherche de séquences d'[Détection étendue des menaces](#) attaques, puis les types de découverte de chaque plan de protection (par ordre alphabétique par plan). Dans le tableau suivant, les valeurs de la colonne de gravité de certains résultats sont marquées d'un astérisque (*) ou d'un signe plus (+) :

* Ces types de résultats ont une gravité variable. Une constatation d'un type particulier peut avoir une gravité différente en fonction du contexte spécifique à la constatation. Pour plus d'informations sur un type de recherche, consultez sa description détaillée.

+ Les résultats de l'EC2 qui utilisent les journaux de flux VPC comme source de données ne prennent pas en charge le trafic IPv6.

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail événement s de gestion	Moyenne
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail événement s de gestion	Moyenne
DefenseEvasion:IAMUser/BedrockLoggingDisabled	IAM	CloudTrail événement s de gestion	Moyenne
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail événement s de gestion	Faible

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail événements de gestion	Élevée
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail événements de gestion	Élevée
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail événements de gestion	Moyenne
PenTest:IAMUser/KaliLinux	IAM	CloudTrail événements de gestion	Moyenne
PenTest:IAMUser/ParrrotLinux	IAM	CloudTrail événements de gestion	Moyenne
PenTest:IAMUser/PentooLinux	IAM	CloudTrail événements de gestion	Moyenne
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail événements de gestion	Moyenne
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail événements de gestion	Faible *
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail événements de gestion	Élevé *
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail événements de gestion	Faible

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail événements de gestion	Élevée
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail événements de gestion	Faible
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail événements de gestion	Élevée
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail événements de gestion	Moyenne
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail événements de gestion	Moyenne
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail événements de gestion	Moyenne
Recon:IAMUser/TorIPCaller	IAM	CloudTrail événements de gestion	Moyenne
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail événements de gestion	Faible
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail événements de gestion	Faible
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail événements de gestion	Moyenne

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail événement s de gestion	Moyenne
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail événement s de gestion	Moyenne
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail événement s de gestion	Moyenne
CredentialAccess:IAMUser/CompromisedCredentials	IAM	CloudTrail événement s de gestion ou événements de CloudTrail données pour S3	Élevée
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail événement s de gestion ou événements de CloudTrail données pour S3	Faible
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	CloudTrail événement s de gestion ou événements de CloudTrail données pour S3	Faible
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail événement s de gestion ou événements de CloudTrail données pour S3	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	IAM	CloudTrail événements de gestion ou événements de CloudTrail données pour S3	Élevée
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	IAM	CloudTrail événement s de gestion ou événements de CloudTrail données pour S3	Élevée
Impact:EC2/MaliciousDomainRequest.Custom	Amazon EC2	Journaux DNS	Moyenne
Backdoor:EC2/C&CAActivity.B!DNS	Amazon EC2	Journaux DNS	Élevée
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Journaux DNS	Élevée
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Journaux DNS	Moyenne
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Journaux DNS	Élevée
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Journaux DNS	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Journaux DNS	Faible
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Journaux DNS	Moyenne
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DropPoint!DNS	Amazon EC2	Journaux DNS	Moyenne
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Journaux DNS	Élevée
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Journaux DNS	Élevée
Backdoor:EC2/C&CActivity.B	Amazon EC2	Journaux de flux VPC +	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Backdoor:EC2/DenialOfService.Dns	Amazon EC2	Journaux de flux VPC +	Élevée
Backdoor:EC2/DenialOfService.Tcp	Amazon EC2	Journaux de flux VPC +	Élevée
Backdoor:EC2/DenialOfService.Udp	Amazon EC2	Journaux de flux VPC +	Élevée
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	Amazon EC2	Journaux de flux VPC +	Élevée
Backdoor:EC2/DenialOfService.UnusualProtocol	Amazon EC2	Journaux de flux VPC +	Élevée
Backdoor:EC2/Spambot	Amazon EC2	Journaux de flux VPC +	Moyenne
Behavior:EC2/NetworkPortUnusual	Amazon EC2	Journaux de flux VPC +	Moyenne
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	Journaux de flux VPC +	Moyenne
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	Journaux de flux VPC +	Élevée
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	Journaux de flux VPC +	Moyenne
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	Journaux de flux VPC +	Moyenne

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	Journaux de flux VPC +	Moyenne
Impact:EC2/PortSweep	Amazon EC2	Journaux de flux VPC +	Élevée
Impact:EC2/WinRMBruteForce	Amazon EC2	Journaux de flux VPC +	Faible [*] ₋
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	Journaux de flux VPC +	Élevée
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	Journaux de flux VPC +	Faible [*] ₋
Recon:EC2/Portscan	Amazon EC2	Journaux de flux VPC +	Moyenne
Trojan:EC2/BlackholeTraffic	Amazon EC2	Journaux de flux VPC +	Moyenne
Trojan:EC2/DropPoint	Amazon EC2	Journaux de flux VPC +	Moyenne
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	Journaux de flux VPC +	Moyenne
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	Journaux de flux VPC +	Faible [*] ₋
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	Journaux de flux VPC +	Faible [*] ₋

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
UnauthorizedAccess:EC2/TorClient	Amazon EC2	Journaux de flux VPC +	Élevée
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	Journaux de flux VPC +	Élevée
AttackSequence:EKS/CompromisedCluster	Ressources impliquées dans la séquence d'attaque	<ul style="list-style-type: none"> • Événements du journal d'audit EKS • Surveillance du temps d'exécution pour Amazon EKS • Détection de malwares Amazon EKS pour Amazon EC2 • AWS CloudTrail l'événements de données pour S3 • AWS CloudTrail l'événements de gestion • Journaux de flux VPC • Journaux de requêtes DNS de Route53 Resolver 	Critique
AttackSequence:IAM/CompromisedCredentials	Ressources impliquées dans la séquence d'attaque	CloudTrail événements de gestion	Critique

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
AttackSequence:S3/CompromisedData	Ressources impliquées dans la séquence d'attaque	CloudTrail événements de gestion et événements de CloudTrail données pour S3	Critique
AttackSequence:ECS/CompromisedCluster	Ressources impliquées dans la séquence d'attaque	<ul style="list-style-type: none"> • AWS Détections d'Amazon ECS Runtime (Fargate) • AWS Détections d'Amazon ECS Runtime (instances Amazon EC2) • AWS Détections de logiciels malveillants 	Critique
AttackSequence:EC2/CompromisedInstanceGroup	Ressources impliquées dans la séquence d'attaque	<ul style="list-style-type: none"> • AWS Détections d'Amazon EC2 Runtime • AWS Détections de logiciels malveillants • Journaux de flux VPC • Journaux de requêtes DNS de Route53 Resolver 	Critique
Impact:IAMUser/AnomalousModelInvocation	IAM	Protection de l'IA	Faible

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Impact:IAMUser/CostHarvesting	IAM	Protection de l'IA	Faible
Impact:IAMUser/ProptInjection.Direct	IAM	Protection de l'IA	Faible
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Journaux d'audit EKS	Moyenne
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Élevée
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Élevée
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Élevée
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Journaux d'audit EKS	Faible
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Moyenne
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Moyenne
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Moyenne
Discovery:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Moyenne
Execution:Kubernetes/ExecInKubernetesPod	Kubernetes	Journaux d'audit EKS	Moyenne
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Journaux d'audit EKS	Moyenne

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Journaux d'audit EKS	Faible
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Élevée
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Élevée
Impact:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Moyenne
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Moyenne
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Élevée
Persistence:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Moyenne
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Journaux d'audit EKS	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Journaux d'audit EKS	Élevée
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Journaux d'audit EKS	Moyenne
Policy:Kubernetes/ExposedDashboard	Kubernetes	Journaux d'audit EKS	Moyenne
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Journaux d'audit EKS	Moyen [*] __
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Journaux d'audit EKS	Faible
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Journaux d'audit EKS	Élevée
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Journaux d'audit EKS	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Backdoor:Lambda/C&CActivity.B	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
Trojan:Lambda/BlackholeTraffic	Lambda	Surveillance de l'activité du réseau Lambda	Moyenne
Trojan:Lambda/DropPoint	Lambda	Surveillance de l'activité du réseau Lambda	Moyenne
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Surveillance de l'activité du réseau Lambda	Moyenne
UnauthorizedAccess:Lambda/TorClient	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
UnauthorizedAccess:Lambda/TorRelay	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
Execution:Container/MaliciousFile	Conteneur	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:Container/SuspiciousFile	Conteneur	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Execution:EC2/MaliciousFile	Amazon EC2	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:EC2/SuspiciousFile	Amazon EC2	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:ECS/MaliciousFile	ECS	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:ECS/SuspiciousFile	ECS	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:Kubernetes/MaliciousFile	Kubernetes	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:Kubernetes/SuspiciousFile	Kubernetes	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:EC2/MaliciousFile!Snapshot	Amazon EBS	Protection contre les logiciels malveillants pour Backup	Varie en fonction de la menace détectée
Execution:EC2/MaliciousFile!AMI	Amazon EC2	Protection contre les logiciels malveillants pour Backup	Varie en fonction de la menace détectée
Execution:EC2/MaliciousFile!Recovery Point	AWS Backup	Protection contre les logiciels malveillants pour Backup	Varie en fonction de la menace détectée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Execution:S3/MaliciousFile!RecoveryPoint	AWS Backup	Protection contre les logiciels malveillants pour Backup	Varie en fonction de la menace détectée
Object:S3/MaliciousFile	S3Object	Protection contre les logiciels malveillants pour S3	Élevée
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Faible
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Élevée
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Variable [*]
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Moyenne

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Élevée
CredentialAccess:RDS/TorIPCaller.FailedLogin	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Moyenne
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Élevée
Discovery:RDS/MaliciousIPCaller	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Moyenne
Discovery:RDS/TorIPCaller	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de connexion RDS	Moyenne
Exfiltration:RDS/AnomalousBehavior	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Faible [*] ₋

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Exfiltration:RDS/MaliciousIPCaller	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Élevée
Exfiltration:RDS/TorIPCaller	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Élevée
Impact:RDS/AnomalousBehavior.Delete	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Faible [*] __
Impact:RDS/AnomalousBehavior.Drop	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Moyen [*] __
Impact:RDS/MaliciousIPCaller	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Élevée
Impact:RDS/TorIPCaller	Bases de données Amazon Aurora, Amazon RDS et Aurora Limitless prises en charge	Surveillance de l'activité de la base de données RDS	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail événements de données pour S3	Faible
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail événements de données pour S3	Élevée
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail événements de données pour S3	Moyenne
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail événements de données pour S3	Élevée
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail événements de données pour S3	Élevée
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail événements de données pour S3	Élevée
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail événements de données pour S3	Moyenne
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
PenTest:S3/KaliLinux	Amazon S3	CloudTrail événements de données pour S3	Moyenne
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail événements de données pour S3	Moyenne

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
PenTest:S3/PentoolLinux	Amazon S3	CloudTrail événements de données pour S3	Moyenne
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail événements de données pour S3	Élevée
Backdoor:Runtime/C&CActivity.B	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Backdoor:Runtime/C&CActivity.B!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
CryptoCurrency:Runtime/BitcoinTool.B	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/FilelessExecution	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
DefenseEvasion:Runtime/KernelModuleLoaded	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
DefenseEvasion:Runtime/SensitiveFileModified	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
DefenseEvasion:Runtime/ProcessInjection.Proc	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/PtraceAntiDebugging	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Faible
DefenseEvasion:Runtime/SuspiciousCommand	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Discovery:Runtime/SuspiciousCommand	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Faible
Execution:Runtime/MaliciousFileExecuted	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Execution:Runtime/MaliciousFileExecuted.Custom	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Execution:Runtime/NewBinaryExecuted	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Execution:Runtime/NewLibraryLoaded	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Execution:Runtime/SuspiciousCommand	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Variable
Execution:Runtime/SuspiciousShellCreated	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Faible
Execution:Runtime/SuspiciousTool	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Variable
Execution:Runtime/ReverseShell	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/AbusedDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Impact:Runtime/BitcoinDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/CryptominerExecuted	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Impact:Runtime/MaliciousDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Faible
Persistence:Runtime/SuspiciousCommand	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Persistence:Runtime/SensitiveFileModified	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
PrivilegeEscalation:Runtime/ElevationToRoot	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
PrivilegeEscalation:Runtime/RuncContainerEscape	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
PrivilegeEscalation:Runtime/SuspiciousCommand	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
PrivilegeEscalation:Runtime/SensitiveFileModified	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
PrivilegeEscalation:Runtime/UserfaultUsage	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Trojan:Runtime/BlackholeTraffic	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Trojan:Runtime/BlackholeTraffic! DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Trojan:Runtime/DropPoint	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne
Trojan:Runtime/DGA DomainRequest.C! DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Trojan:Runtime/DriveBySourceTraffic! DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Trojan:Runtime/DropPoint! DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Moyenne

Type de résultat	Type de ressource	Données de base source/Feature	Gravité du résultat
Trojan:Runtime/PhishingDomainRequest!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/TorClient	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/TorRelay	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Comprendre et générer des GuardDuty résultats sur Amazon

Une GuardDuty découverte représente un problème de sécurité potentiel détecté dans Comptes AWS les charges de travail et les données. GuardDuty génère un résultat chaque fois qu'il détecte une activité inattendue et potentiellement malveillante dans votre AWS environnement.

Vous pouvez consulter et gérer vos GuardDuty résultats sur la page Résultats de la GuardDuty console, ou en utilisant les opérations de l'API AWS CLI ou. Pour plus d'informations sur la façon dont vous pouvez gérer GuardDuty les résultats, consultez [Gérer les GuardDuty résultats d'Amazon](#).

Rubriques :

[GuardDuty format de recherche](#)

Comprenez le format de GuardDuty recherche des types de menaces et les différents objectifs du GuardDuty suivi.

[Exemples de résultats](#)

Générez des exemples de résultats dans la GuardDuty console ou à l'aide de l' GuardDuty API ou AWS CLI des commandes. Les échantillons de résultats générés incluent des détails fictifs pour vous aider à comprendre les détails associés à chaque GuardDuty résultat. Ces résultats sont marqués d'un préfixe [SAMPLE].

[GuardDuty Résultats des tests dans des comptes dédiés](#)

Vous pouvez tester des GuardDuty résultats spécifiques dans votre environnement. Exécutez `guardduty-tester` le script dans un espace dédié à la non-production Compte AWS. GuardDuty Pour détecter et simuler les résultats, il déploiera certaines ressources dans votre environnement. Cette expérience est différente de la production d'échantillons de résultats.

[Affichage des résultats générés dans la GuardDuty console](#)

Découvrez comment consulter les résultats générés dans la GuardDuty console.

[Niveaux de gravité des GuardDuty résultats](#)

Chaque GuardDuty découverte est associée à un niveau de gravité qui reflète le risque potentiel dans votre AWS environnement. Cette section explique ce que signifie chaque niveau de gravité.

[Détails d'un résultat](#)

Découvrez les détails associés aux GuardDuty résultats générés sur votre compte. Cette rubrique inclut les détails associés à la détection fondamentale des menaces, à la détection étendue des menaces et aux plans de protection dédiés dans GuardDuty.

[GuardDuty recherche d'agrégation](#)

Découvrez comment GuardDuty gérer plusieurs occurrences du même type de recherche. En agrégeant les mêmes types de résultats détectés, GuardDuty met à jour le type de résultat d'origine avec les informations les plus récentes.

[GuardDuty types de recherche](#)

Cette section répertorie les types de GuardDuty recherche en fonction de la valeur associée [Source de données de base](#) ou [Fonctionnalité mappée GuardDuty](#). Pour en savoir plus sur chaque type de constatation, sélectionnez cette constatation pour plus de détails, tels que sa description et les mesures possibles pour y remédier.

GuardDuty format de recherche

Lorsqu' GuardDuty un comportement suspect ou inattendu est détecté dans votre AWS environnement, il génère une constatation. Une constatation est une notification qui contient les détails d'un problème de sécurité potentiel GuardDuty découvert. Ils [Affichage des résultats générés dans la GuardDuty console](#) incluent des informations sur ce qui s'est passé, les AWS ressources impliquées dans l'activité suspecte, le moment où cette activité a eu lieu, ainsi que des informations connexes susceptibles de vous aider à en comprendre la cause première.

Le type de résultat est l'une des informations les plus utiles. Le type de résultat vise à fournir une description brève mais intelligible du problème de sécurité potentiel. Par exemple, le type de GuardDuty Recon:EC2/PortProbeUnprotectedPortrecherche vous informe rapidement que quelque part dans votre AWS environnement, une instance EC2 possède un port non protégé qu'un attaquant potentiel est en train de tester.

GuardDuty utilise le format suivant pour nommer les différents types de résultats qu'il génère :

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism! Artifact

Chaque partie de ce format représente un aspect d'un type de résultat. Ces aspects sont expliqués comme suit :

- **ThreatPurpose**- décrit l'objectif principal d'une menace, le type d'attaque ou le stade d'une attaque potentielle. Consultez la section suivante pour obtenir une liste complète des objectifs GuardDuty liés aux menaces.
- **ResourceTypeAffected**- décrit le type de AWS ressource identifié dans cette constatation comme étant la cible potentielle d'un adversaire. Actuellement, GuardDuty peut générer des résultats pour les types de ressources répertoriés dans le [GuardDuty types de recherche actifs](#).
- **ThreatFamilyName**- décrit la menace globale ou l'activité malveillante potentielle GuardDuty détectée. Par exemple, une valeur de `NetworkPortUnusual` indique qu'une instance EC2 identifiée dans la GuardDuty recherche n'a aucun historique de communications sur un port distant particulier qui est également identifié dans la recherche.
- **DetectionMechanism**- décrit la méthode utilisée pour GuardDuty détecter le résultat. Cela peut être utilisé pour indiquer une variation par rapport à un type de découverte courant ou un résultat qui a GuardDuty utilisé un mécanisme de détection spécifique. Par exemple, `Backdoor:EC2/DenialOfService.Tcp` indique qu'un déni de service (DoS) a été détecté via TCP. La variante UDP est `Backdoor:EC2/DenialOfService.Udp`.

La valeur `.Custom` indique que le résultat a GuardDuty été détecté sur la base de vos listes de menaces personnalisées. Pour de plus amples informations, veuillez consulter [Listes d'entités et listes d'adresses IP](#).

La valeur `.Reputation` indique que le résultat a GuardDuty été détecté à l'aide d'un modèle de score de réputation de domaine. Pour plus d'informations, consultez [How AWS suit les principales menaces de sécurité du cloud et aide à les neutraliser](#).

- **Artefact** : décrit une ressource spécifique appartenant à un outil utilisé pour l'activité malveillante. Par exemple, le DNS dans le type de recherche [CryptoCurrency:EC2/BitcoinTool.B!DNS](#) indique qu'une instance Amazon EC2 communique avec un domaine connu Bitcoin-related .

Note

L'Artefact est facultatif et peut ne pas être disponible pour tous les types de GuardDuty recherche.

Buts de la menace

Dans GuardDuty une menace, l'objectif décrit l'objectif principal d'une menace, un type d'attaque ou un stade d'une attaque potentielle. Par exemple, certaines menaces, telles que Backdoor,

indiquent un type d'attaque. Cependant, certains buts de la menace, tels que Impact, s'alignent sur les [tactiques MITRE ATT&CK](#). Les tactiques MITRE ATT&CK indiquent les différentes phases du cycle d'attaque d'un adversaire. Dans la version actuelle de GuardDuty, ThreatPurpose peut avoir les valeurs suivantes :

Backdoor

Cette valeur indique qu'un adversaire a compromis une AWS ressource et l'a modifiée afin de pouvoir contacter son serveur central de commande et de contrôle (C&C) pour recevoir des instructions supplémentaires concernant une activité malveillante.

Comportement

Cette valeur indique que l'on GuardDuty a détecté une activité ou des modèles d'activité différents de la base de référence établie pour les AWS ressources impliquées.

CredentialAccess

Cette valeur indique qu'il GuardDuty a détecté des modèles d'activité qu'un adversaire pourrait utiliser pour voler des informations d'identification, telles que des mots de passe, des noms d'utilisateur et des clés d'accès, dans votre environnement. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Cryptomonnaie

Cette valeur indique qu' GuardDuty une AWS ressource de votre environnement héberge un logiciel associé à des cryptomonnaies (par exemple, Bitcoin).

DefenseEvasion

Cette valeur indique qu'il GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire peut utiliser pour éviter d'être détecté lors de l'infiltration de votre environnement. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Découverte

Cette valeur indique qu'il GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire pourrait utiliser pour approfondir ses connaissances de vos systèmes et de vos réseaux internes. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Exécution

Cette valeur indique qu'un adversaire GuardDuty a détecté qu'un adversaire essaie d'exécuter ou a déjà exécuté un code malveillant pour explorer l' AWS environnement ou pour voler des données. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Exfiltration

Cette valeur indique qu'il GuardDuty a détecté une activité ou des modèles d'activité susceptibles d'être utilisés par un adversaire pour tenter de voler des données dans votre environnement. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Impact

Cette valeur indique qu'une activité ou des modèles d'activité ont GuardDuty été détectés qui suggèrent qu'un adversaire tente de manipuler, d'interrompre ou de détruire vos systèmes et vos données. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

InitialAccess

Cette valeur est généralement associée à la phase d'accès initiale d'une attaque lorsqu'un adversaire tente d'accéder à votre environnement. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Pentest

Parfois, les propriétaires de AWS ressources ou leurs représentants autorisés exécutent intentionnellement des tests sur AWS des applications pour détecter des vulnérabilités, telles que des groupes de sécurité ouverts ou des clés d'accès trop permissives. Ces tests d'intrusion sont réalisés pour tenter d'identifier et de verrouiller les ressources vulnérables avant qu'elles ne soient découvertes par des adversaires. Toutefois, certains des outils utilisés par les testeurs autorisés sont disponibles gratuitement et peuvent donc être utilisés par des utilisateurs non autorisés ou des adversaires à des fins d'analyse. Bien qu'il ne soit pas GuardDuty possible d'identifier le véritable objectif d'une telle activité, la valeur GuardDuty Pentest indique qu'il s'agit de détecter une telle activité, qu'elle est similaire à celle générée par des outils de test de stylet connus et qu'elle pourrait indiquer une enquête malveillante sur votre réseau.

Persistence

Cette valeur indique qu'il GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire peut utiliser pour tenter de conserver l'accès à vos systèmes même si sa voie d'accès initiale est coupée. Par exemple, cela peut inclure la création d'un utilisateur IAM après avoir obtenu l'accès via les informations d'identification compromises d'un utilisateur existant. Lorsque les informations d'identification de l'utilisateur existant sont supprimées, l'adversaire retient l'accès au nouvel utilisateur qui n'a pas été détecté lors de l'événement d'origine. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Stratégie

Cette valeur indique que votre comportement Compte AWS va à l'encontre des meilleures pratiques de sécurité recommandées. Par exemple, modification involontaire des politiques d'autorisation associées à vos AWS ressources ou à votre environnement, et utilisation de comptes privilégiés qui devraient être peu ou pas utilisés.

PrivilegeEscalation

Cette valeur vous indique que le principal impliqué dans votre environnement AWS présente un comportement susceptible d'être utilisé par un adversaire pour obtenir des autorisations de niveau supérieur sur votre réseau. Ce but de la menace est basé sur les [tactiques MITRE ATT&CK](#).

Recon

Cette valeur indique qu'il GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire peut utiliser lors de la reconnaissance de votre environnement afin de déterminer comment il peut élargir son accès ou utiliser vos ressources. Par exemple, cette activité peut inclure l'identification des vulnérabilités de votre AWS environnement en analysant les ports, en effectuant des appels d'API, en répertoriant les utilisateurs et en répertoriant les tables de base de données, entre autres.

Stealth

Cette valeur indique qu'un adversaire essaie activement de masquer ses actions. Par exemple, il peut utiliser un serveur proxy anonyme, ce qui rend extrêmement difficile l'évaluation de la véritable nature de l'activité.

Trojan

Cette valeur indique qu'une attaque utilise des chevaux de Troie pour mener une action malveillante en silence. Parfois, ce logiciel prend l'aspect d'un programme légitime. Parfois, les utilisateurs l'exécutent accidentellement. Ou bien le logiciel peut s'exécuter automatiquement en exploitant une vulnérabilité.

UnauthorizedAccess

Cette valeur indique qu'une activité suspecte ou un schéma d'activité suspect GuardDuty est détecté par une personne non autorisée.

GuardDuty moteur d'analyse pour la détection des malwares

Amazon GuardDuty dispose d'un moteur de scan conçu et géré en interne et d'un [fournisseur tiers](#). Les deux utilisent des indicateurs de compromission (IoCs) provenant de différents flux internes qui permettent de visualiser les différents types de malwares susceptibles de les cibler AWS. GuardDuty propose également des définitions de détection basées sur les règles YARA ajoutées par nos ingénieurs en sécurité, ainsi que des détections basées sur des modèles heuristiques et d'apprentissage automatique (ML). Lors de l'analyse d'objets Amazon S3, GuardDuty Malware Protection produit des résultats cohérents en scannant le même objet plusieurs fois avec les mêmes définitions et moteurs de scan. Signature-based la détection inclut non seulement la mise en correspondance d'octets, mais également un extrait de code potentiellement complexe, et le scanner peut analyser le contenu et prendre des décisions.

Le moteur d'analyse des programmes malveillants n'effectue pas d'analyse comportementale en temps réel, dans le cadre de laquelle la détonation du logiciel malveillant surveille l'échantillon lorsqu'il s'exécute dans un système réel. La GuardDuty solution consiste principalement en une détection basée sur des fichiers. Pour détecter les malwares sans fichier, GuardDuty fournit une solution basée sur un agent, telle que pour [Surveillance d'exécution](#) Amazon EKS, Amazon EC2 et Amazon ECS (y compris). AWS Fargate

Sans aucune restriction quant aux formats de fichiers permettant de détecter les malwares, les moteurs d'analyse qu'il utilise peuvent détecter différents types de malwares, tels que les cryptomineurs, les ransomwares et les webshells. GuardDuty Le moteur d' GuardDuty analyse entièrement géré met à jour en permanence la liste des signatures de logiciels malveillants toutes les 15 minutes.

Le moteur d'analyse fait partie d'un système de renseignement sur les GuardDuty menaces qui utilise un composant interne de détonation de logiciels malveillants. Cela génère de nouvelles informations sur les menaces en collectant indépendamment des malwares et des échantillons bénins provenant de sources multiples. Le type de hachage de fichier IoC du système de renseignement sur les menaces alimente également le moteur d'analyse des logiciels malveillants afin de détecter les logiciels malveillants sur la base de hachages de fichiers défectueux connus.

Génération d'échantillons de résultats dans GuardDuty

Amazon vous GuardDuty aide à générer des échantillons de résultats afin de visualiser et de comprendre les différents types de résultats qu'il peut générer. Lorsque vous générez des résultats

d'échantillonnage, GuardDuty renseigne votre liste de résultats actuelle avec un échantillon pour chaque type de découverte pris en charge, y compris les types de recherche de séquences d'attaque.

Les exemples générés sont des approximations renseignées avec des valeurs d'espace réservé. Ces exemples peuvent sembler différents des résultats réels pour votre environnement, mais vous pouvez les utiliser pour tester différentes configurations GuardDuty, telles que vos EventBridge événements ou vos filtres. Pour obtenir la liste des valeurs disponibles pour rechercher des types, consultez le [GuardDuty types de recherche](#) tableau.

Génération d'échantillons de résultats via la GuardDuty console ou l'API

Choisissez votre méthode d'accès préférée pour générer des exemples de résultats.

Note

La GuardDuty console vous permet de générer un résultat pour chaque type de recherche. Pour générer un ou plusieurs types de résultats spécifiques, effectuez les API/CLI étapes associées.

Console

Utilisez la procédure suivante pour générer des exemples de résultats. Ce processus génère un échantillon de résultats pour chaque type de GuardDuty résultat.

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Settings, sous Sample findings, choisissez Generate sample findings.
4. Dans le volet de navigation, choisissez Conclusions. Les exemples de résultats sont affichés sur la page Résultats actuels avec le préfixe [SAMPLE].

API/CLI

Vous pouvez générer un seul échantillon correspondant à n'importe quel type de GuardDuty résultat via l'[CreateSampleFindings](#) API. Les valeurs disponibles pour les types de recherche sont répertoriées dans le [GuardDuty types de recherche](#) tableau.

Ceci est utile pour tester les règles relatives aux CloudWatch événements ou l'automatisation en fonction des résultats. L'exemple suivant montre comment générer un exemple de résultat unique du type `Backdoor:EC2/DenialOfService.Tcp` à l'aide de l' AWS CLI.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
--finding-types Backdoor:EC2/DenialOfService.Tcp
```

Le titre des exemples de résultats générés par ces méthodes commence toujours par [SAMPLE] dans la console. Les exemples de résultats ont une valeur de "sample": true dans la section additionalInfo des détails JSON du résultat.

Pour comprendre les détails des résultats, tels que la gravité de la découverte et la ressource potentiellement compromise, associés aux résultats générés, voir [Niveaux de gravité des GuardDuty résultats](#) et [Détails d'un résultat](#).

Pour générer des résultats courants sur la base d'une activité simulée dans un environnement dédié et isolé Compte AWS de votre environnement, consultez [GuardDuty Résultats des tests dans des comptes dédiés](#).

GuardDuty Résultats des tests dans des comptes dédiés

Utilisez ce document pour exécuter un script de test qui génère des GuardDuty résultats par rapport aux ressources de test qui seront déployées dans votre Compte AWS. Vous pouvez effectuer ces étapes pour comprendre et en savoir plus sur certains types de GuardDuty recherche, ainsi que sur la manière dont les informations de recherche correspondent aux ressources réelles de votre compte. Cette expérience est différente de la génération [Exemples de résultats](#). Pour plus d'informations sur l'expérience des GuardDuty résultats des tests, consultez [Considérations](#).

Table des matières

- [Considérations](#)
- [GuardDuty résultats que le script de testeur peut générer](#)
- [Étape 1 - Prérequis](#)
- [Étape 2 - Déployer AWS les ressources](#)

- [Étape 3 - Exécuter des scripts de test](#)
- [Étape 4 - Nettoyer les ressources AWS de test](#)
- [Dépannage des problèmes courants](#)

Considérations

Avant de poursuivre, tenez compte des considérations suivantes :

- GuardDuty recommande de déployer le testeur dans un environnement de non-production Compte AWS dédié. Cette approche vous permettra d'identifier correctement les GuardDuty résultats générés par le testeur. En outre, le GuardDuty testeur déploie diverses ressources qui peuvent nécessiter des autorisations IAM au-delà de ce qui est autorisé dans d'autres comptes. L'utilisation d'un compte dédié garantit que les autorisations peuvent être correctement définies avec des limites de compte claires.
- Le script du testeur génère plus de 100 GuardDuty résultats avec différentes combinaisons de AWS ressources. Actuellement, cela n'inclut pas tous les [GuardDuty types de recherche](#). Pour obtenir la liste des types de recherche que vous pouvez générer avec ce script de test, consultez [GuardDuty résultats que le script de testeur peut générer](#).

Remarque

Pour visualiser les types de recherche de séquences d'attaque, le script du testeur génère uniquement [AttackSequence:EKS/CompromisedCluster](#) et [AttackSequence:S3/CompromisedData](#). Pour visualiser et comprendre [AttackSequence:IAM/CompromisedCredentials](#), vous pouvez le générer [Exemples de résultats](#) dans votre compte.

- Pour que le GuardDuty testeur fonctionne comme prévu, il GuardDuty doit être activé dans le compte sur lequel les ressources du testeur sont déployées. En fonction des tests à exécuter, le testeur évalue si les plans de GuardDuty protection appropriés sont activés ou non. Pour tout plan de protection qui n'est pas activé, GuardDuty vous demanderez l'autorisation d'activer les plans de protection nécessaires suffisamment longtemps GuardDuty pour effectuer les tests qui généreront des résultats. Plus tard, le plan de protection GuardDuty sera désactivé une fois le test terminé.
- Activation GuardDuty pour la première fois

Lorsqu' GuardDuty il est activé sur votre compte dédié pour la première fois dans une région spécifique, votre compte sera automatiquement inscrit à un essai gratuit de 30 jours.

GuardDuty propose des plans de protection optionnels. Au moment de l'activation GuardDuty, certains plans de protection sont également activés et sont inclus dans l'essai gratuit de GuardDuty 30 jours. Pour de plus amples informations, veuillez consulter [Utilisation de l' GuardDuty essai gratuit de 30 jours](#).

GuardDuty est déjà activé dans votre compte avant l'exécution du script de test

Lorsque cette option GuardDuty est déjà activée, le script du testeur vérifie l'état de configuration de certains plans de protection et d'autres paramètres au niveau du compte requis pour générer les résultats en fonction des paramètres.

En exécutant ce script de test, certains plans de protection peuvent être activés pour la première fois sur votre compte dédié dans une région. Cela lancera l'essai gratuit de 30 jours pour ce plan de protection. Pour plus d'informations sur l'essai gratuit associé à chaque plan de protection, consultez [Utilisation de l' GuardDuty essai gratuit de 30 jours](#).

- Tant que l'infrastructure du GuardDuty testeur est déployée, vous pouvez parfois recevoir [UnauthorizedAccess:EC2/TorClient](#) les résultats de l' PenTest instance.

GuardDuty résultats que le script de testeur peut générer

Actuellement, le script du testeur génère les types de résultats suivants liés aux journaux d'audit Amazon EC2, Amazon EKS, Amazon S3, IAM et EKS :

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:S3/CompromisedData](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)

- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [PenTest:IAMUser/KaliLinux](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)

- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)
- [Backdoor:Runtime/C&CActivity.B! DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B! DNS](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [Trojan:Runtime/BlackholeTraffic! DNS](#)
- [Trojan:Runtime/DGADomainRequest.C! DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic! DNS](#)
- [Trojan:Runtime/DropPoint! DNS](#)
- [Trojan:Runtime/PhishingDomainRequest! DNS](#)

Étape 1 - Prérequis

Pour préparer votre environnement de test, vous aurez besoin des éléments suivants :

- Git — Installez l'outil de ligne de commande git en fonction du système d'exploitation que vous utilisez.

Cela est nécessaire pour cloner le [amazon-guardduty-tester](#)dépôt.

- AWS Command Line Interface— Un outil open source avec lequel vous pouvez interagir à l'aide Services AWS de commandes dans votre interface de ligne de commande. Pour plus

d'informations, voir [Commencer AWS CLI](#) dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Systems Manager— Pour lancer des sessions de gestionnaire de session avec vos nœuds gérés en utilisant, AWS CLI vous devez installer le plug-in Session Manager sur votre machine locale. Pour plus d'informations, voir [Installer le plug-in Session Manager AWS CLI](#) dans le guide de AWS Systems Manager l'utilisateur.
- Node Package Manager (NPM) — Installez NPM pour installer toutes les dépendances.
- Docker — Docker doit être installé. Pour obtenir les instructions d'installation, consultez le [site web Docker](#).

Pour vérifier que Docker a été installé, exécutez la commande suivante et vérifiez qu'il existe un résultat similaire au résultat suivant :

```
$ docker --version
Docker version 19.03.1
```

- Abonnez-vous à l'image [Kali Linux](#) dans le AWS Marketplace.

Étape 2 - Déployer AWS les ressources

Cette section fournit une liste des concepts clés et les étapes à suivre pour déployer certaines AWS ressources dans votre compte dédié.

Concepts

La liste suivante fournit les concepts clés liés aux commandes qui vous aident à déployer les ressources :

- Cloud Development Kit AWS (AWS CDK)— CDK est un framework de développement de logiciels open source permettant de définir l'infrastructure cloud dans le code et de la provisionner via celui-ci. CloudFormation CDK prend en charge plusieurs langages de programmation pour définir des composants cloud réutilisables appelés constructions. Vous pouvez les composer ensemble en piles et en applications. Vous pouvez ensuite déployer vos applications CDK pour approvisionner ou mettre CloudFormation à jour vos ressources. Pour plus d'informations, voir [Qu'est-ce que le AWS CDK ?](#) dans le Guide Cloud Development Kit AWS (AWS CDK) du développeur.
- Bootstrapping — Il s'agit du processus de préparation de votre AWS environnement pour une utilisation avec. AWS CDK Avant de déployer une pile CDK dans un AWS environnement, celui-ci doit d'abord être amorcé. Ce processus de mise en service de AWS ressources spécifiques dans

vos environnements qui sont utilisés par AWS CDK fait partie des étapes que vous allez effectuer dans la section suivante - [Étapes de déploiement AWS des ressources](#).

Pour plus d'informations sur le fonctionnement du bootstrapping, voir [Bootstrapping](#) dans le manuel du développeur.Cloud Development Kit AWS (AWS CDK)

Étapes de déploiement AWS des ressources

Procédez comme suit pour commencer à déployer les ressources :

1. Configurez votre compte et votre région AWS CLI par défaut, sauf si les variables de région du compte dédié sont définies manuellement dans le `bin/cdk-gd-tester.ts` fichier. Pour plus d'informations, consultez la section [Environnements](#) du guide du Cloud Development Kit AWS (AWS CDK) développeur.
2. Exécutez les commandes suivantes pour déployer les ressources :

```
git clone https://github.com/aws-labs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

La dernière commande (`cdk deploy`) crée une CloudFormation pile en votre nom. Le nom de cette pile est `GuardDutyTesterStack`.

Dans le cadre de ce script, GuardDuty crée de nouvelles ressources pour générer des GuardDuty résultats dans votre compte. Il ajoute également la paire de balises clé:valeur suivante aux instances Amazon EC2 :

`CreatedBy:GuardDuty Test Script`

Les instances Amazon EC2 incluent également les instances EC2 qui hébergent des nœuds EKS et des clusters ECS.

Types d'instances

GuardDuty est conçu pour utiliser des types d'instances économiques qui fournissent les performances minimales nécessaires pour mener à bien les tests. En raison des exigences en matière de vCPU, le groupe de nœuds Amazon EKS en a besoin `t3.medium`, et en

raison de l'augmentation de la capacité réseau requise pour la DenialOfService recherche de tests, le nœud pilote en a besoin. `m6i.1large` Pour tous les autres tests, GuardDuty utilise le type d'instance `t3.micro`. Pour plus d'informations sur les types d'instances, consultez la section [Tailles disponibles](#) dans le guide des types d'instances Amazon EC2.

Étape 3 - Exécuter des scripts de test

Il s'agit d'un processus en deux étapes dans lequel vous devez d'abord démarrer une session avec le pilote de test, puis exécuter des scripts pour générer des GuardDuty résultats avec des combinaisons de ressources spécifiques.

Partie A - Démarrer une session avec le pilote d'essai

1. Une fois vos ressources déployées, enregistrez le code de région dans une variable dans votre session de terminal en cours. Utilisez la commande suivante et remplacez-la `us-east-1` par le code de région dans lequel vous avez déployé les ressources :

```
$ REGION=us-east-1
```

2. Le script du testeur n'est disponible que via AWS Systems Manager (SSM). Pour démarrer un shell interactif sur l'instance hôte du testeur, interrogez l'hôte `InstanceId`.
3. Utilisez la commande suivante pour démarrer votre session pour le script du testeur :

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

Partie B - Générer des résultats

Le script testeur est un Python-based programme qui crée dynamiquement un script bash pour générer des résultats en fonction de vos entrées. Vous disposez de la flexibilité nécessaire pour générer des résultats basés sur un ou plusieurs types de AWS ressources, plans de GuardDuty

protection [Source de données de base](#), [Buts de la menace](#) (tactiques) ou [the section called "GuardDuty résultats que le script de testeur peut générer"](#).

Utilisez les exemples de commandes suivants comme référence et exécutez une ou plusieurs commandes pour générer les résultats que vous souhaitez explorer :

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Pour plus d'informations sur les paramètres valides, vous pouvez exécuter la commande d'aide suivante :

```
python3 guardduty_tester.py --help
```

Partie C - Conclusions générées par l'examen

Choisissez une méthode préférée pour afficher les résultats générés dans votre compte.

GuardDuty console

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans le tableau des résultats, sélectionnez un résultat dont vous souhaitez consulter les détails. Cela ouvrira le panneau des détails de la recherche. Pour plus d'informations, consultez [Comprendre et générer des GuardDuty résultats sur Amazon](#).
4. Si vous souhaitez filtrer ces résultats, utilisez la clé et la valeur de la balise de ressource. Par exemple, pour filtrer les résultats générés pour les instances Amazon EC2, utilisez **CreatedBy : GuardDuty Test Script** tag key:value pair pour la clé de balise d'instance et la clé de balise d'instance.

API

- Exécutez [ListFindings](#) pour afficher les résultats d'un identifiant de détecteur spécifique. Vous pouvez définir des paramètres pour filtrer les résultats.

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

AWS CLI

- Exécutez la AWS CLI commande suivante pour afficher les résultats générés et remplacez *us-east-1* et par *12abc34d567e8fa901bc2d34EXAMPLE* des valeurs appropriées :

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```

`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

Pour plus d'informations sur les paramètres que vous pouvez utiliser pour filtrer les résultats, consultez [list-findings](#) dans la référence des AWS CLI commandes.

Étape 4 - Nettoyer les ressources AWS de test

Les paramètres au niveau du compte et les autres mises à jour de l'état de configuration effectuées lors du [Étape 3 - Exécuter des scripts de test](#) retour à l'état d'origine à la fin du script du testeur.

Après avoir exécuté le script du testeur, vous pouvez choisir de nettoyer les ressources de AWS test. Vous pouvez choisir de le faire en utilisant l'une des méthodes suivantes :

- Exécutez la commande suivante :

```
cdk destroy
```

- Supprimez la CloudFormation pile portant le nom GuardDutyTesterStack. Pour plus d'informations sur les étapes, voir [Supprimer une pile sur la CloudFormation console](#).

Dépannage des problèmes courants

GuardDuty a identifié les problèmes courants et recommande les étapes de résolution des problèmes :

- `Cloud assembly schema version mismatch`— Mettez à jour la AWS CDK CLI vers une version compatible avec la version d'assemblage cloud requise ou vers la dernière version disponible. Pour plus d'informations, consultez la section [Compatibilité avec les AWS CDK CLI](#).
- `Docker permission denied`— Ajoutez l'utilisateur du compte dédié au docker ou aux docker-users afin que le compte dédié puisse exécuter les commandes. Pour plus d'informations sur les étapes, consultez l'[option Daemon socket](#).
- `Your requested instance type is not supported in your requested Availability Zone`— Certaines zones de disponibilité ne prennent pas en charge certains types d'instances. Pour identifier les zones de disponibilité compatibles avec votre type d'instance préféré et réessayer de déployer AWS des ressources, effectuez les opérations suivantes :
 1. Choisissez une méthode préférée pour déterminer les zones de disponibilité compatibles avec votre type d'instance :

Console

Pour identifier les zones de disponibilité qui prennent en charge le type d'instance préféré

1. Connectez-vous à la console Amazon EC2 Console de gestion AWS et ouvrez-la à l'adresse. <https://console.aws.amazon.com/ec2/>
2. À l'aide du sélecteur de AWS région situé dans le coin supérieur droit de la page, choisissez la région dans laquelle vous souhaitez lancer l'instance.
3. Dans le volet de navigation, sous Instances, sélectionnez Types d'instances.
4. Dans le tableau Types d'instances, choisissez un type d'instance préféré.
5. Sous Mise en réseau, consultez les régions répertoriées sous Zones de disponibilité.

Sur la base de ces informations, vous devrez peut-être choisir une nouvelle région dans laquelle vous pourrez déployer les ressources.

AWS CLI

Exécutez la commande suivante pour afficher la liste des zones de disponibilité. Assurez-vous de spécifier votre type d'instance préféré et la région (*us-east-1*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone --  
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --  
output table
```

Pour plus d'informations sur cette commande, consultez [describe-instance-type-offerings](#) dans la référence des commandes.AWS CLI

Lorsque vous exécutez cette commande, si vous recevez un message d'erreur, assurez-vous que vous utilisez la dernière version de AWS CLI. Pour plus d'informations, consultez [Résolution des problèmes](#) dans le Guide de l'utilisateur AWS Command Line Interface .

2. Réessayez de déployer les AWS ressources et spécifiez une zone de disponibilité qui prend en charge votre type d'instance préféré.

Pour réessayer de déployer des ressources AWS

1. Configurez la région par défaut dans le `bin/cdk-gd-tester.ts` fichier.
2. Pour définir la zone de disponibilité, ouvrez le `amazon-guardduty-tester/lib/common/network/vpc.ts` fichier.
3. Dans ce fichier, remplacez `maxAzs: 2`, par `availabilityZones: ['us-east-1a', 'us-east-1c']`, endroit où vous devez spécifier les zones de disponibilité pour votre type d'instance.
4. Continuez avec les étapes restantes ci-dessous [Étapes de déploiement AWS des ressources](#).

Affichage des résultats générés dans la GuardDuty console

Lorsqu'il GuardDuty détecte une activité qui correspond au schéma d'un problème de sécurité, GuardDuty génère un résultat. Cette découverte est associée à un type de ressource qui peut avoir été compromis au cours de cette activité. Vous pouvez consulter les détails associés à chaque résultat GuardDuty généré.

Si vous utilisez un compte GuardDuty administrateur, vous pouvez consulter les résultats générés pour le compte des membres. Cependant, un compte membre peut consulter les résultats générés sur son propre compte. Un compte membre ne peut pas consulter les résultats générés pour les autres comptes membres.

Étapes pour afficher les résultats dans GuardDuty la console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation de gauche, choisissez Findings.

GuardDuty affiche les résultats sous forme de tableau. Par défaut, ce tableau est trié par ordre décroissant en fonction de la valeur de la colonne Dernière vue, affichant les résultats les plus récents en haut.

Les résultats marqués d'une icône en forme d'épée



représentent la découverte d'une séquence d'attaque.

3. Pour afficher les détails associés à une découverte, sélectionnez son titre. Cela ouvrira le panneau latéral des détails de la recherche. Pour trouver une séquence d'attaque, ce panneau latéral inclut une version résumée de la séquence d'attaque, et pour développer cette vue, choisissez Afficher les détails.

Pour plus d'informations sur les champs répertoriés dans ce panneau latéral, consultez [Détails d'un résultat](#).

4. (Facultatif) pour télécharger Finding JSON
 - a. Sélectionnez le résultat, puis choisissez le menu Actions.
 - b. Dans le menu Actions, choisissez Afficher et exporter le JSON.
 - c. Dans la fenêtre Findings JSON, choisissez Télécharger.

Note

Dans certains cas, GuardDuty se rend compte que certains résultats sont des faux positifs une fois qu'ils ont été générés. GuardDuty fournit un champ de confiance dans le JSON de la découverte et définit sa valeur sur zéro. De cette façon GuardDuty , vous savez que vous pouvez ignorer ces résultats en toute sécurité.

Les résultats sans le champ de confiance ne sont pas considérés comme des faux positifs.

Navigation dans la page des résultats

Cette section fournit des informations clés sur les différents éléments de la page Résultats. Cela vous aidera à analyser les résultats générés à des fins d'analyse et de réponse aux menaces.

La liste suivante décrit les éléments de la page Résultats qui vous aideront à mieux comprendre les résultats générés :

- Type de menace :

Le type de menace inclut GuardDuty les résultats individuels et les résultats de la séquence d'attaque. Par défaut, la page affiche Tous les résultats.

Pour filtrer l'affichage du tableau des résultats, dans le menu Type de menace, choisissez l'une des options : Résultats de la séquence d'attaque uniquement ou Résultats individuels uniquement.

- Colonnes Ressources et Nombre :

La colonne Ressource du tableau des résultats indique le nom de la AWS ressource potentiellement compromise. Pour la détection d'une séquence d'attaque, cette colonne indique le nombre de AWS ressources potentiellement compromises. Pour afficher les noms des ressources, sélectionnez le numéro dans la colonne Ressource.

La colonne Nombre indique le nombre de fois où GuardDuty un résultat spécifique est observé. Lorsqu'il GuardDuty détecte qu'une activité correspond à un problème de sécurité précédemment identifié, il augmente le nombre correspondant à ce résultat spécifique. Pour la détection d'une séquence d'attaque, cette valeur de colonne indique le nombre total de signaux et de résultats impliqués dans la génération de la découverte.

- Tri des résultats par colonnes de tableau :

Si une flèche apparaît à côté de l'en-tête d'une colonne, vous pouvez trier le tableau des résultats en fonction de la colonne. Sélectionnez l'en-tête de colonne pour trier les résultats par ordre croissant ou décroissant de la valeur de cette colonne.

- Résultats du filtrage :

En fonction d'attributs de propriété spécifiques, tels que Account ID etResource type, vous pouvez filtrer davantage le tableau des résultats. Pour plus d'informations sur les types de filtres que vous pouvez utiliser, consultez [Filtrer GuardDuty les résultats](#).

- Statut et règles enregistrées :

Le menu **État** comprend deux valeurs : **Actuel** et **Archivé**. L'affichage par défaut est **Les résultats actuels** du tableau.

Lorsque vous ne souhaitez plus GuardDuty générer un résultat correspondant à un critère spécifique, vous pouvez supprimer ce résultat. GuardDuty archive cette découverte. Lorsque ce résultat sera GuardDuty détecté à nouveau, vous ne serez pas averti de cette observation. Pour afficher spécifiquement les résultats archivés, dans le menu **État**, choisissez **Archivé**.

Les règles enregistrées sont une fonctionnalité qui vous permet de filtrer automatiquement les résultats qui correspondent à des critères spécifiques et de prendre des mesures en conséquence. Les actions peuvent inclure l'archivage des résultats ou leur suppression des notifications futures.

Pour de plus amples informations, veuillez consulter [Règles de suppression](#).

Niveaux de gravité des GuardDuty résultats

Chaque GuardDuty découverte est associée à un niveau de gravité et à une valeur qui reflètent le risque potentiel que cette découverte pourrait présenter pour votre environnement, tel que déterminé par nos ingénieurs en sécurité. La valeur de gravité peut se situer n'importe où dans la plage de 1,0 à 10,0, les valeurs les plus élevées indiquant un risque de sécurité accru. Pour vous aider à déterminer la réponse à apporter à un problème de sécurité potentiel mis en évidence par une découverte, GuardDuty répartissez cette plage en niveaux de gravité **critique**, **élevé**, **moyen** et **faible**.

Une constatation d'un type particulier peut avoir une gravité différente selon le contexte spécifique à la découverte. Pour consulter une liste consolidée des niveaux de gravité par défaut pour tous les GuardDuty types de détection, consultez [GuardDuty types de recherche actifs](#).

Les sections suivantes expliquent les niveaux de gravité définis pour les GuardDuty résultats.

Rubriques

- [Gravité critique](#)
- [Gravité élevée](#)
- [Gravité moyenne](#)
- [Faible gravité](#)

Gravité critique

Plage de valeurs : 9,0 - 10,0

Description : Un niveau de gravité critique indique qu'une séquence d'attaque est peut-être en cours ou s'est produite récemment. Une ou plusieurs AWS ressources, telles que les informations de connexion utilisateur IAM et le compartiment Amazon S3, sont potentiellement compromises ou l'ont peut-être déjà été.

Recommandation : vous GuardDuty recommande de donner la priorité au tri et à la correction de tous les problèmes de gravité critiques, car ces problèmes peuvent être liés à une attaque de rançongiciel et peuvent s'aggraver à tout moment. Consultez les détails des ressources concernées et commencez à résoudre les problèmes de sécurité. Pour de plus amples informations, veuillez consulter [Correction des résultats](#).

Gravité élevée

Plage de valeurs : 7,0 - 8,9

Description : Un niveau de gravité élevé indique que la ressource en question (une instance Amazon EC2 ou un ensemble d'informations de connexion utilisateur IAM) est compromise et est activement utilisée à des fins non autorisées.

Recommandation : vous GuardDuty recommande de traiter en priorité tout problème de sécurité lié à la détection d'un niveau de gravité élevé et de prendre des mesures correctives immédiates pour empêcher toute nouvelle utilisation non autorisée de vos ressources. Par exemple, nettoyez votre instance Amazon EC2 ou mettez-la hors service, ou modifiez les informations d'identification IAM. Suivez les étapes décrites [Correction des résultats](#) pour remédier à cette constatation.

Gravité moyenne

Plage de valeurs : 4,0 - 6,9

Description : Un niveau de gravité moyen indique une activité suspecte qui s'écarte du comportement normalement observé et, selon votre cas d'utilisation, peut indiquer une compromission des ressources.

Recommandation : GuardDuty recommande d'étudier la ressource potentiellement affectée dans les meilleurs délais. Les mesures correctives varient en fonction de la ressource et de la famille de recherche. Une approche d'établissement vous permet de confirmer que l'activité est autorisée et conforme à votre cas d'utilisation. Si vous ne pouvez pas identifier la cause ou confirmer que l'activité

a été autorisée, vous devez considérer que la ressource est compromise. Suivez les étapes décrites [Correction des résultats](#) pour remédier à cette constatation.

Voici quelques éléments à prendre en compte lors de l'examen d'un résultat de niveau moyen :

- Vérifiez si un utilisateur autorisé a installé un nouveau logiciel qui a changé le comportement d'une ressource (par exemple, trafic plus élevé que le trafic normal autorisé ou communication activée sur un nouveau port).
- Vérifiez si un utilisateur autorisé a modifié les paramètres du plan de contrôle, par exemple un paramètre de groupe de sécurité.
- Exécutez une analyse antivirus sur les ressources impliquées pour détecter les logiciels non autorisés.
- Vérifiez les autorisations qui sont attachées au rôle IAM impliqué, à l'utilisateur, au groupe ou à l'ensemble d'informations d'identification. Celles-ci peuvent avoir été modifiées ou fait l'objet d'une rotation.

Faible gravité

Plage de valeurs : 1,0 - 3,9

Description : Un niveau de gravité faible indique une tentative d'activité suspecte qui n'a pas compromis votre environnement, par exemple un scan de port ou une tentative d'intrusion ratée.

Recommandation : Aucune action immédiate n'est recommandée, mais il vaut la peine de prendre note de ces informations car elles peuvent indiquer que quelqu'un recherche les points faibles de votre environnement.

Détails d'un résultat

Dans la GuardDuty console Amazon, vous pouvez consulter les détails des recherches dans la section récapitulative des recherches. Les détails des résultats varient en fonction du type de résultat.

Deux détails principaux permettent de déterminer les types d'information disponibles pour tout résultat. Le premier est le type de ressource, qui peut être Instance, AccessKey, S3Bucket, S3Object, Kubernetes cluster, ECS cluster, Container, RDSDBInstance, RDSLimitlessDB, ou Lambda. Le deuxième détail qui détermine les informations d'un résultat est le rôle de la ressource. Le rôle de la ressource peut être Target tel que la ressource a été la cible d'une activité suspecte. Pour les résultats du type

d'instance, le rôle de la ressource peut également être `Actor`, ce qui signifie que votre ressource était l'acteur à l'origine de l'activité suspecte. Cette rubrique décrit certains des détails les plus fréquemment disponibles en matière de résultats. Pour [the section called “Types de recherche liés à la surveillance du temps”](#) et [Protection contre les programmes malveillants pour le type de recherche S3](#), le rôle de ressource n'est pas renseigné.

Rubriques

- [Présentation des résultats](#)
- [Ressource](#)
- [Détails de recherche de la séquence d'attaque](#)
- [Règles de détection personnalisées pour trouver des détails](#)
- [Détails de l'utilisateur de base de données \(DB\) RDS](#)
- [Surveillance d'exécution : détails des résultats](#)
- [Détails de l'analyse des volumes EBS](#)
- [Protection contre les logiciels malveillants pour la recherche de détails dans EC2](#)
- [Informations sur la recherche effectuée par la protection contre les logiciels malveillants pour S3](#)
- [Action](#)
- [Acteur ou cible](#)
- [Détails de géolocalisation](#)
- [Informations supplémentaires](#)
- [Preuve](#)
- [Comportement anormal](#)

Présentation des résultats

La section Présentation d'un résultat contient les fonctionnalités d'identification les plus élémentaires du résultat, notamment les informations suivantes :

- **ID du compte** : identifiant du AWS compte sur lequel s'est déroulée l'activité qui a incité GuardDuty à générer ce résultat.
- **Nombre** : nombre de fois qu'une activité correspondant à ce modèle GuardDuty a été agrégée à cet identifiant de recherche.
- **Créé à** : heure et date de création de ce résultat. Si cette valeur diffère de la valeur Mise à jour à, cela indique que l'activité s'est produite plusieurs fois et qu'il s'agit d'un problème continu.

 Note

Les horodatages des résultats dans la GuardDuty console apparaissent dans votre fuseau horaire local, tandis que les exportations JSON et les sorties CLI affichent les horodatages en UTC.

- ID de résultat : identifiant unique pour ce type de résultat et ensemble de paramètres. Les nouvelles occurrences d'activité correspondant à ce modèle seront regroupées sous le même ID.
- Type de résultat : chaîne formatée représentant le type d'activité qui a déclenché le résultat. Pour plus d'informations, consultez [GuardDuty format de recherche](#).
- Région : AWS région dans laquelle le résultat a été généré. Pour de plus amples informations sur les régions prises en charge, veuillez consulter [Régions et points de terminaison](#).
- ID de ressource : ID de la AWS ressource par rapport à laquelle a eu lieu l'activité qui a incité GuardDuty à générer ce résultat.
- ID de scan : applicable aux résultats lorsque la protection contre les GuardDuty programmes malveillants pour EC2 est activée, il s'agit d'un identifiant de l'analyse des programmes malveillants exécutée sur les volumes EBS attachés à l'instance ou à la charge de travail du conteneur EC2 potentiellement compromise. Pour plus d'informations, consultez [Protection contre les logiciels malveillants pour la recherche de détails dans EC2](#).
- Gravité : niveau de gravité attribué à un résultat : critique, élevé, moyen ou faible. Pour plus d'informations, consultez [Niveaux de gravité des résultats](#).
- Mis à jour à — La dernière fois que ce résultat a été mis à jour avec une nouvelle activité correspondant au modèle qui a incité GuardDuty à générer ce résultat.

Ressource

La ressource affectée fournit des détails sur la AWS ressource ciblée par l'activité initiatrice. Les informations disponibles varient selon le type de ressource et le type d'action.

Rôle de ressource : rôle de la AWS ressource à l'origine de la recherche. Cette valeur peut être CIBLE ou ACTEUR, et indique si votre ressource était la cible de l'activité suspecte ou l'acteur qui a effectué l'activité suspecte.

Type de ressource : type de la ressource affectée. Si plusieurs ressources étaient impliquées, un résultat peut inclure plusieurs types de ressource. Les types de ressources sont Instance, S3Bucket

AccessKey, S3Object, ECSCluster, Container, RDSDBInstance KubernetesCluster, RDSLimitlessDB et Lambda. Selon le type de ressource, différents détails de résultats sont disponibles. Sélectionnez un onglet d'option de ressource pour en savoir plus sur les détails disponibles pour cette ressource.

Instance

Détails de l'instance :

Note

Certains détails de l'instance peuvent être manquants si l'instance a déjà été arrêtée ou si l'invocation d'API sous-jacente provient d'une instance EC2 d'une autre région lors d'un appel d'API entre régions.

- ID d'instance : ID de l'instance EC2 impliquée dans l'activité qui a incité GuardDuty à générer le résultat.
- Type d'instance : type de l'instance EC2 impliquée dans le résultat.
- Heure de lancement : date et heure auxquelles l'instance a été lancée.
- Outpost ARN — Le nom de ressource Amazon (ARN) de AWS Outposts. Applicable uniquement aux AWS Outposts instances. Pour plus d'informations, voir [Qu'est-ce que c'est AWS Outposts ?](#) dans le Guide de l'utilisateur pour les racks Outposts.
- Nom du groupe de sécurité : nom du groupe de sécurité attaché à l'instance concernée.
- ID du groupe de sécurité : ID du groupe de sécurité attaché à l'instance concernée.
- État de l'instance : état actuel de l'instance ciblée.
- Zone de disponibilité : zone de disponibilité de la Région AWS dans laquelle se trouve l'instance concernée.
- ID de l'image : ID de l'Amazon Machine Image utilisée pour créer l'instance impliquée dans l'activité.
- Description de l'image : description de l'ID de l'Amazon Machine Image utilisée pour créer l'instance impliquée dans l'activité.
- Balises : liste des balises attachées à cette ressource, répertoriées au format key:value.

AccessKey

Détails de la clé d'accès :

- ID de clé d'accès : ID de clé d'accès de l'utilisateur impliqué dans l'activité GuardDuty à l'origine de la recherche.
- ID principal : identifiant principal de l'utilisateur impliqué dans l'activité GuardDuty à l'origine de la recherche.
- Type d'utilisateur : type d'utilisateur impliqué dans l'activité qui a incité GuardDuty à générer le résultat. Pour de plus amples informations, veuillez consulter [Élément CloudTrail userIdentity](#).
- Nom d'utilisateur : nom de l'utilisateur impliqué dans l'activité GuardDuty à l'origine de la recherche.

S3Bucket

Détails du compartiment Amazon S3 :

- Nom : nom du compartiment impliqué dans le résultat.
- ARN : ARN du compartiment impliqué dans le résultat.
- Propriétaire : ID utilisateur canonique de l'utilisateur propriétaire du compartiment impliqué dans le résultat. Pour de plus amples informations sur l'ID d'utilisateur canonique, veuillez consulter [Identificateurs de compte AWS](#).
- Type : le type de résultat de compartiment peut être Destination ou Source.
- Détails du chiffrement côté serveur par défaut : détails du chiffrement pour le compartiment.
- Balises de compartiment : liste des balises attachées à cette ressource, répertoriées au format `key:value`.
- Autorisations effectives : évaluation de toutes les autorisations et stratégies effectives sur le compartiment qui indique si le compartiment impliqué est exposé publiquement. Les valeurs peuvent être Publique ou Non publique.

S3Object

- Détails de l'objet S3 : inclut les informations suivantes sur l'objet S3 scanné :
 - ARN — Nom de ressource Amazon (ARN) de l'objet S3 scanné.
 - Clé : nom attribué au fichier lors de sa création dans le compartiment S3.
 - ID de version : lorsque vous avez activé le contrôle de version des compartiments, ce champ indique l'identifiant de version associé à la dernière version de l'objet S3 scanné. Pour plus d'informations, consultez la section [Utilisation du versionnement dans les compartiments S3](#) dans le guide de l'utilisateur Amazon S3.

- ETag — Représente la version spécifique de l'objet S3 scanné.
- Hachage : hachage de la menace détectée dans cette constatation.
- Détails du compartiment S3 : inclut les informations suivantes sur le compartiment Amazon S3 associé à l'objet S3 scanné :
 - Nom — Indique le nom du compartiment S3 contenant l'objet.
 - ARN — Nom de ressource Amazon (ARN) du compartiment S3.
- Propriétaire : identifiant canonique du propriétaire du compartiment S3.

EKSCluster

Détails du cluster Kubernetes :

- Nom : nom du cluster Kubernetes.
- ARN : l'ARN qui identifie le cluster.
- Créé à : heure et date de création de ce cluster.

Note

Les horodatages des résultats dans la GuardDuty console apparaissent dans votre fuseau horaire local, tandis que les exportations JSON et les sorties CLI affichent les horodatages en UTC.

- ID de VPC : ID du VPC associé à votre cluster.
- État : extrait l'état actuel du cluster.
- Balises : métadonnées que vous appliquez au cluster pour faciliter le classement et l'organisation. Chaque balise est constituée d'une clé et d'une valeur facultative, répertoriées au format `key:value`. Vous pouvez définir à la fois la clé et la valeur.

Les balises de cluster ne sont pas propagées vers les autres ressources associées au cluster.

Détails de la charge de travail Kubernetes :

- Type : type de charge de travail Kubernetes, tel que le pod, le déploiement et la tâche.
- Nom : nom de la charge de travail Kubernetes.
- Uid : identifiant unique de la charge de travail Kubernetes.

- Créé à : heure et date de création de cette charge de travail.
- Étiquettes : paires clé-valeur attachées à la charge de travail Kubernetes.
- Conteneurs : détails du conteneur exécuté dans le cadre de la charge de travail de Kubernetes.
- Espace de noms : la charge de travail appartient à cet espace de noms Kubernetes.
- Volumes : volumes utilisés par la charge de travail Kubernetes.
 - Chemin d'accès de l'hôte : représente un fichier ou un répertoire préexistant sur la machine hôte vers lequel le volume est mappé.
 - Nom : nom du volume.
- Contexte de sécurité du pod : définit les paramètres de contrôle des privilèges et des accès pour tous les conteneurs d'un pod.
- Réseau hôte : définissez sur `true` si les pods sont inclus dans la charge de travail Kubernetes.

Informations utilisateur Kubernetes :

- Groupes : groupes de RBAC (contrôle basé sur l'accès aux rôles) de Kubernetes de l'utilisateur qui participe à l'activité qui a généré le résultat.
- ID : ID unique de l'utilisateur Kubernetes.
- Nom d'utilisateur : nom de l'utilisateur Kubernetes qui participe à l'activité à l'origine du résultat.
- Nom de session : entité qui a assumé le rôle IAM avec les autorisations RBAC de Kubernetes.

ECSCluster

Détails du cluster ECS :

- ARN : l'ARN qui identifie le cluster.
- Nom : nom du cluster.
- État : extrait l'état actuel du cluster.
- Nombre de services actifs : nombre de services exécutés sur le cluster à l'état ACTIVE. Vous pouvez consulter ces services avec [ListServices](#)
- Nombre d'instances de conteneur enregistrées : nombre d'instances de conteneur enregistrées dans le cluster. Cela inclut les instances de conteneur à la fois à l'état ACTIVE et DRAINING.
- Nombre de tâches en cours : nombre de tâches du cluster qui sont à l'état RUNNING.

- Balises : métadonnées que vous appliquez au cluster pour faciliter le classement et l'organisation. Chaque balise est constituée d'une clé et d'une valeur facultative, répertoriées au format `key:value`. Vous pouvez définir à la fois la clé et la valeur.
- Conteneurs : détails sur le conteneur associé à la tâche :
 - Nom de conteneur : nom du conteneur.
 - Image de conteneur : image du conteneur.
- Détails de la tâche : détails d'une tâche dans un cluster.
 - ARN : Amazon Resource Name (ARN) de la tâche.
 - ARN de la définition : Amazon Resource Name (ARN) de la définition de tâche qui crée la tâche.
 - Version : compteur de version de la tâche.
 - Tâche créée à : horodatage Unix lors de la création de la tâche.
 - Tâche démarrée à : horodatage Unix lors du démarrage d'une tâche.
 - Tâche démarrée par : balise spécifiée lors du démarrage d'une tâche.

Container

Détails du conteneur :

- Exécution du conteneur : exécution du conteneur (comme `docker` ou `containerd`) utilisé pour exécuter le conteneur.
- ID : ID de l'instance de conteneur ou entrées ARN complètes pour l'instance de conteneur.
- Nom : nom du conteneur.
- Image : image de l'instance de conteneur.
- Montages de volume : liste des montages de volume de conteneurs. Un conteneur peut monter un volume sous son système de fichiers.
- Contexte de sécurité : le contexte de sécurité du conteneur définit les paramètres de contrôle de privilèges et d'accès pour un conteneur.
- Détails du processus : décrit les détails du processus associé au résultat.

RDSDBInstance

Détails de l'instance RDSDB :

 Note

Cette ressource est disponible dans les résultats de protection RDS relatifs à l'instance de base de données.

- ID de l'instance de base de données : identifiant associé à l'instance de base de données impliquée dans la GuardDuty recherche.
- Moteur : nom du moteur de base de données de l'instance de base de données impliquée dans le résultat. Les valeurs possibles sont Aurora MySQL-Compatible ou Aurora PostgreSQL-Compatible.
- Version du moteur : version du moteur de base de données impliquée dans la GuardDuty recherche.
- ID du cluster de base de données : identifiant du cluster de base de données qui contient l'identifiant de l'instance de base de données impliquée dans la GuardDuty recherche.
- ARN de l'instance de base de données : ARN identifiant l'instance de base de données impliquée dans la GuardDuty recherche.

RDSLimitlessDB

Détails de RDSLimitlessDB :

Cette ressource est disponible dans les résultats de protection RDS relatifs à la version du moteur prise en charge de Limitless Database.

- Identifiant du groupe de partitions de base de données : nom associé au groupe de partitions de base de données Limitless.
- ID de ressource du groupe de partitions de base de données : identifiant de ressource du groupe de partitions de base de données au sein de la base de données Limitless.
- ARN du groupe de partitions de base de données — Le nom de ressource Amazon (ARN) qui identifie le groupe de partitions de base de données.
- Moteur — Identifiant de la base de données Limitless impliquée dans la recherche.
- Version du moteur : version du moteur de base de données Limitless.
- Identifiant du cluster de base de données : nom du cluster de base de données qui fait partie de la base de données Limitless.

Pour plus d'informations sur les informations relatives à l'utilisateur et à l'authentification de la base de données potentiellement affectée, consultez [Détails de l'utilisateur de base de données \(DB\) RDS](#).

Lambda

Détails de la fonction Lambda

- Nom de la fonction : nom de la fonction Lambda impliquée dans le résultat.
- Version de la fonction : version de la fonction Lambda impliquée dans le résultat.
- Description de la fonction : description de la fonction Lambda impliquée dans le résultat.
- ARN de fonction : Amazon Resource Name (ARN) de la fonction Lambda impliquée dans le résultat.
- ID de révision : ID de révision de la version de la fonction Lambda.
- Rôle : rôle d'exécution de la fonction Lambda impliquée dans le résultat.
- Configuration de VPC : configuration d'Amazon VPC, y compris l'ID VPC, le groupe de sécurité et les ID de sous-réseau associés à votre fonction Lambda.
 - ID de VPC : ID d'Amazon VPC associé à la fonction Lambda impliquée dans le résultat.
 - ID de sous-réseau : ID des sous-réseaux associés à votre fonction Lambda.
 - Groupe de sécurité : groupe de sécurité attaché à la fonction Lambda concernée. Cela inclut le nom et l'ID du groupe de sécurité.
- Balises : liste des balises attachées à cette ressource, répertoriées au format de paire `key:value`.

Détails de recherche de la séquence d'attaque

GuardDuty fournit des informations détaillées sur chaque recherche générée dans votre compte. Ces informations vous aident à comprendre les raisons de cette découverte. Cette section se concentre sur les détails associés à [Types de détection de séquences d'attaques](#). Cela inclut des informations telles que les ressources potentiellement affectées, la chronologie des événements, les indicateurs, les signaux et les points de terminaison impliqués dans le résultat.

Pour afficher les détails associés aux signaux qui sont des GuardDuty résultats, consultez les sections associées de cette page.

Dans la GuardDuty console, lorsque vous sélectionnez une recherche de séquence d'attaque, le panneau latéral détaillé est divisé en onglets suivants :

- **Vue d'ensemble** : fournit une vue compacte des détails de la séquence d'attaque, y compris les signaux, les tactiques MITRE et les ressources potentiellement touchées.
- **Signaux** : affiche une chronologie des événements impliqués dans une séquence d'attaque.
- **Ressources** — Fournit des informations sur les ressources potentiellement touchées ou les ressources potentiellement menacées.

La liste suivante fournit des descriptions associées aux détails de la recherche de la séquence d'attaque.

Signaux

Un signal peut être une activité d'API ou une découverte GuardDuty utilisée pour détecter une séquence d'attaque. GuardDuty prend en compte les signaux faibles qui ne se présentent pas comme une menace claire, les synthétise et les met en corrélation avec les résultats générés individuellement. Pour plus de contexte, l'onglet Signaux fournit une chronologie des signaux, telle qu'observée par GuardDuty.

Chaque signal, c'est-à-dire une GuardDuty constatation, possède son propre niveau de gravité et sa propre valeur. Dans la GuardDuty console, vous pouvez sélectionner chaque signal pour afficher les détails associés.

Acteurs

Fournit des informations sur les acteurs de la menace dans une séquence d'attaque. Pour plus d'informations, consultez [Actor](#) dans Amazon GuardDuty API Reference.

Points de terminaison

Fournit des détails sur les points de terminaison du réseau utilisés dans cette séquence d'attaque. Pour plus d'informations, consultez [NetworkEndpoint](#) le manuel Amazon GuardDuty API Reference. Pour plus d'informations sur le mode GuardDuty de détermination de l'emplacement, consultez [Détails de géolocalisation](#).

Indicateurs

Inclut les données observées qui correspondent au schéma d'un problème de sécurité. Ces données indiquent pourquoi il existe une indication d'une activité potentiellement suspecte. Par exemple, lorsque le nom de l'indicateur est `HIGH_RISK_API`, cela indique une action couramment utilisée par les auteurs de menaces, ou une action sensible susceptible d'avoir un impact potentiel sur un Compte AWS, comme l'accès aux informations d'identification ou la modification d'une ressource.

Le tableau suivant inclut une liste d'indicateurs potentiels et leurs descriptions :

Nom de l'indicateur	Description
ATTACK_TACTIC	Les tactiques MITRE utilisées par l'auteur de la menace dans une séquence d'attaque. Les exemples incluent Discovery et Impact.
ATTACK_TECHNIQUE	Technique MITRE utilisée par l'auteur de la menace dans une séquence d'attaque. Les exemples incluent l'accès aux ressources et leur utilisation involontaire, ainsi que l'exploitation des vulnérabilités.
CRYPTOMINING_DOMAIN	Indique un nom de domaine associé à des pools ou à une infrastructure de minage de cryptomonnaies. Par exemple, les requêtes DNS ou les connexions à ces domaines depuis des conteneurs ou des environnements Kubernetes peuvent indiquer une activité de cryptomining non autorisée.
CRYPTOMINING_IP	Indique une adresse IP associée aux pools ou à l'infrastructure de minage de cryptomonnaies. Par exemple, les connexions à ces adresses depuis des conteneurs ou des environnements Kubernetes peuvent indiquer une activité de cryptomining non autorisée.
CRYPTOMINING_PROCESS	Indique un processus identifié comme un logiciel d'extraction de cryptomonnaies exécuté dans des environnements de conteneurs ou Kubernetes. Par exemple, ces processus peuvent consommer des ressources CPU excessives.
HIGH_RISK_API	L' AWS API qui inclut le Service AWS nom et eventName indique une action couramment utilisée par les auteurs de menaces, ou qui est une action sensible susceptible d'avoir un impact potentiel sur un Compte AWS, telle que l'accès aux informations d'identification ou la modification des ressources.
MALICIOUS_DOMAIN	Indique un nom de domaine contenant des informations suspectes indiquant une intention malveillante. Cela inclut par exemple les serveurs de commande et de contrôle (C&C), les sites de distribution de logiciels malveillants ou les domaines de phishing contactés depuis des conteneurs ou des environnements Kubernetes.

Nom de l'indicateur	Description
MALICIOUS_FILE	Indique un fichier suspecté d'être malveillant sur la base de renseignements sur les menaces ou d'une analyse comportementale. Cela inclut, par exemple, les fichiers binaires de logiciels malveillants connus, les scripts malveillants ou les exécutables non autorisés.
MALICIOUS_IP	L'adresse IP contient des informations de menace confirmées indiquant une intention malveillante.
MALICIOUS_PACKAGE	Indique qu'une ressource impliquée dans la séquence d'attaque contient un package logiciel identifié comme malveillant. Les valeurs des indicateurs incluent des identificateurs de packages malveillants utilisant la désignation OSV (MAL-*) associée aux packages détectés.
MALICIOUS_PROCESS	Indique un processus soupçonné d'être malveillant sur la base de renseignements sur les menaces ou d'une analyse comportementale. Cela inclut, par exemple, les malwares connus, les portes dérobées ou les outils non autorisés s'exécutant dans un environnement d'instance ou de conteneur.
MISCONFIGURATION	Indique qu'une ressource impliquée dans la séquence d'attaque présente une configuration de sécurité défectueuse susceptible d'en augmenter l'impact potentiel. Les exemples incluent les politiques d'accès administratif, le versionnement désactivé ou le chiffrement manquant. Ces erreurs de configuration sont identifiées par AWS Security Hub CSPM. Pour plus d'informations, consultez la section Types de traits pris en charge dans le guide de AWS Security Hub CSPM l'utilisateur.
REACHABILITY	Indique qu'une ressource impliquée dans la séquence d'attaque est accessible depuis Internet ou est accessible au public. Les exemples incluent les instances Amazon EC2 accessibles par Internet, les clusters Amazon EKS, les clusters Amazon ECS ou les compartiments Amazon S3 accessibles au public. Pour plus d'informations, consultez la section Types de traits pris en charge dans le guide de AWS Security Hub CSPM l'utilisateur.

Nom de l'indicateur	Description
SENSITIVE_DATA	Indique qu'un compartiment Amazon S3 impliqué dans la séquence d'attaque contient des données sensibles, telles qu'identifiées par Amazon Macie via. AWS Security Hub CSPM
SUSPICIOUS_NETWORK	Le réseau est associé à de faibles scores de réputation connus, tels que des fournisseurs de réseaux privés virtuels (VPN) risqués et des services de proxy.
SUSPICIOUS_PROCESS	Indique un processus suspect identifié comme anormal sur la base de renseignements sur les menaces ou d'une analyse comportementale. Cela inclut, par exemple, des modèles d'exécution de processus inhabituels, des relations parent-enfant inattendues ou des processus présentant des caractéristiques suspectes au sein d'une instance ou d'un environnement de conteneur.
SUSPICIOUS_USER_AGENT	L'agent utilisateur est associé à des applications suspectes ou exploitées potentiellement connues, telles que les clients Amazon S3 et les outils d'attaque.
TOR_IP	L'adresse IP est associée à un nœud de sortie Tor.
UNUSUAL_API_FOR_ACCOUNT	Indique que l' AWS API a été invoquée de manière anormale, sur la base de référence historique du compte. Pour plus d'informations, consultez Comportement anormal .
UNUSUAL_ASIN_FOR_ACCOUNT	Indique que le numéro de système autonome (ASN) a été identifié comme anormal, sur la base de référence historique du compte. Pour plus d'informations, consultez Comportement anormal .
UNUSUAL_ASIN_FOR_USER	Indique que le numéro de système autonome (ASN) a été identifié comme anormal, sur la base de la référence historique de l'utilisateur. Pour plus d'informations, consultez Comportement anormal .

Nom de l'indicateur	Description
VULNERABILITY	Indique qu'une ressource impliquée dans la séquence d'attaque présente des vulnérabilités connues de gravité critique, élevée, moyenne ou faible. Les valeurs des indicateurs incluent les identifiants CVE et leurs niveaux de gravité. Ces vulnérabilités sont détectées par Amazon Inspector et peuvent augmenter l'impact potentiel de la séquence d'attaque. Pour plus d'informations sur les niveaux de gravité, consultez Comprendre les niveaux de gravité dans le guide de l'utilisateur d'Amazon Inspector.

Tactiques MITRE

Ce champ indique les tactiques MITRE ATT&CK utilisées par l'auteur de la menace au cours d'une séquence d'attaque. GuardDuty utilise le framework [MITRE ATT&ACK](#) qui ajoute du contexte à l'ensemble de la séquence d'attaque. Les couleurs utilisées par la GuardDuty console pour spécifier les objectifs de menace utilisés par l'auteur de la menace s'alignent sur les couleurs indiquant les niveaux critique, élevé, moyen et faible [Niveaux de gravité des résultats](#).

Indicateurs de réseau

Les indicateurs incluent une combinaison de valeurs d'indicateurs de réseau qui expliquent pourquoi un réseau est révélateur d'un comportement suspect. Cette section s'applique uniquement lorsque l'indicateur inclut SUSPICIOUS_NETWORK ou MALICIOUS_IP. L'exemple suivant montre comment les indicateurs de réseau peuvent être associés à un indicateur, où :

- *AnyCompany* est un système autonome (AS).
- TUNNEL_VPNIS_ANONYMOUS, et ALLOWS_FREE_ACCESS sont les indicateurs du réseau.

```
...{
  "key": "SUSPICIOUS_NETWORK",
  "values": [{
    "AnyCompany": [
      "TUNNEL_VPN",
      "IS_ANONYMOUS",
      "ALLOWS_FREE_ACCESS"
    ]
  }]
}
```

Le tableau suivant inclut les valeurs des indicateurs de réseau et leur description. Ces balises sont ajoutées en fonction des informations sur les menaces GuardDuty collectées auprès de sources telles que Spur.

Valeur de l'indicateur de réseau	Description
TUNNEL_VPN	L'adresse réseau ou IP est associée à un type de tunnel VPN. Il s'agit d'un protocole spécifique qui permet d'établir une connexion sécurisée et cryptée entre deux points sur un réseau public.
TUNNEL_PROXY	L'adresse réseau ou IP est associée à un type de tunnel proxy. Il s'agit d'un protocole spécifique qui permet d'établir une connexion via un serveur proxy.
TUNNEL_RDP	L'adresse réseau ou IP est associée à l'utilisation d'une méthode d'encapsulation du trafic de poste de travail distant (RDP) dans un autre protocole afin d'améliorer la sécurité, de contourner les restrictions du réseau ou de permettre l'accès à distance via des pare-feux.
IS_ANONYMOUS	L'adresse réseau ou IP est associée à un service anonyme ou proxy connu. Cela peut indiquer des activités suspectes potentielles qui se cachent derrière des réseaux anonymes.
KNOWN_THREAT_OPERATOR	L'adresse réseau ou IP est associée à un fournisseur de tunnel connu à risque. Cela indique qu'une activité suspecte a été détectée à partir d'une adresse IP liée à un VPN, à un proxy ou à d'autres services de tunneling fréquemment utilisés à des fins malveillantes.
ALLOWS_FREE_ACCESS	L'adresse réseau ou IP est associée à un opérateur de tunnel qui permet d'accéder à son service sans authentification ni paiement. Cela peut également inclure des comptes d'essai ou des expériences d'utilisation limitées proposées par divers services en ligne.
ALLOWS_CRYPTO	L'adresse réseau ou IP est associée à un fournisseur de tunnel (tel qu'un VPN ou un service proxy) qui accepte exclusivement les cryptomonnaies ou autres monnaies numériques comme mode de paiement.

Valeur de l'indicateur de réseau	Description
ALLOWS_TO_RRENTS	L'adresse réseau ou IP est associée à des services ou à des plateformes qui autorisent le trafic torrent. Ces services sont souvent associés au soutien et à l'utilisation de torrents, ainsi qu'à des activités de contournement des droits d'auteur.
RISK_CALL_BACK_PROXY	L'adresse réseau ou IP est associée à des appareils connus pour acheminer le trafic vers des proxys résidentiels, des proxys malveillants ou d'autres réseaux de type proxy de rappel. Cela ne signifie pas que toutes les activités sur le réseau sont liées au proxy, mais plutôt que le réseau a la capacité d'acheminer le trafic pour le compte de ces réseaux proxy.
RISK_GEO_MISMATCH	Cet indicateur suggère que l'emplacement du centre de données ou de l'hébergement d'un réseau est différent de l'emplacement attendu des utilisateurs et des appareils qui le sous-tendent. Si cette valeur d'indicateur n'est pas présente, cela ne signifie pas qu'il n'y a aucune incompatibilité. Cela peut impliquer que les données sont insuffisantes pour confirmer l'écart.
IS_SCANNER	L'adresse réseau ou IP est associée à des tentatives de connexion persistantes sur des formulaires Web.
RISK_WEB_SCRAPING	Le réseau d'adresses IP est associé aux clients Web automatisés et à d'autres activités Web programmatiques.
CLIENT_BEHAVIOR_FILE_SHARING	L'adresse réseau ou IP est associée au comportement du client indiquant des activités de partage de fichiers, telles que les réseaux poste à poste (P2P) ou les protocoles de partage de fichiers.
CATEGORY_COMMERCIAL_VPN	L'adresse réseau ou IP est associée à un opérateur de tunnel classé comme un service de réseau privé virtuel (VPN) commercial traditionnel opérant dans l'espace d'un centre de données.
CATEGORY_FREE_VPN	L'adresse réseau ou IP est associée à un opérateur de tunnel classé dans la catégorie des services VPN entièrement gratuits.

Valeur de l'indicateur de réseau	Description
CATEGORY_RESIDENTIAL_PROXY	L'adresse réseau ou IP est associée à un opérateur de tunnel classé dans la catégorie SDK, logiciel malveillant ou service proxy rémunéré.
OPERATOR_XXX	Le nom du fournisseur de services qui exploite ce tunnel.

Règles de détection personnalisées pour trouver des détails

Les détails d'une recherche sur les règles de détection personnalisées dépendent de la source de données de la règle qui l'a générée.

Conclusions tirées de AWS CloudTrail rules

Les résultats issus AWS CloudTrail des règles utilisent la même `Service.Detection.Sequence` structure que [Détails de recherche de la séquence d'attaque](#). Les champs `Acteurs`, `Endpoints`, `Resources` et `Signals` partagent le même schéma. Les informations suivantes sont spécifiques aux règles de détection personnalisées.

Type

Le type de recherche suit le format `Tactic:Service/Technique`. Par exemple : `Persistence:EC2/ExternalRemoteServices`.

Signaux

Chaque signal représente un événement de règle unique correspondant. Le `Name` champ contient le nom des règles de détection personnalisées, ainsi `SignalIndicators` que la tactique et la technique MITRE ATT&CK®. Plusieurs signaux associés à la même règle peuvent apparaître lorsque la règle correspond à plusieurs événements dans la fenêtre d'agrégation.

Acteurs

Détails sur les principaux IAM qui ont effectué l'activité détectée. Inclut le type d'utilisateur (tel que `AssumedRole` ou `IAMUser`), les informations d'identification et les détails de la session, notamment l'ARN du rôle émetteur et le statut MFA.

Ressources

Informations sur les AWS ressources impliquées dans l'activité détectée, le cas échéant, telles que les instances Amazon EC2, les compartiments Amazon S3 ou les clés d'accès IAM.

Points de terminaison

Détails sur les points de terminaison du réseau d'où provient l'activité. Comprend l'adresse IP, l'emplacement géographique (ville et pays), ainsi que le nom et le numéro du système autonome (AS).

Résultats des règles de surveillance du temps d'exécution

Les résultats issus des règles de surveillance du temps d'exécution utilisent la même structure que les autres résultats de surveillance du temps d'exécution, y compris les détails d'exécution du processus impliqué. Pour plus d'informations, consultez [Surveillance d'exécution : détails des résultats](#). Les détails suivants sont spécifiques aux règles de détection personnalisées :

Type

Le type de recherche suit le format `Tactic:Runtime/Technique`. Par exemple :
`Persistence:Runtime/SuspiciousCommand`.

Règle

Le `CustomDetectionRuleName` champ contient le nom de la règle de détection personnalisée qui a généré le résultat.

Contexte

Les `Service.RuntimeDetails.Context` champs décrivent l'activité correspondante. Les champs inclus dans une recherche dépendent de la règle :

- Les règles qui génèrent `SensitiveFileRead` et obtiennent `SensitiveFileModified` des résultats incluent `FilePath` et `FileOperation`.
- La plupart des règles qui génèrent des `SuspiciousCommand` résultats incluent `CommandLineExample`, et certaines incluent également `ServiceName`. Les règles qui détectent l'activité sur un fichier spécifique, telles que la modification des autorisations d'un fichier, incluent `FilePath` plutôt et `FileOperation` quand elles s'appliquent.
- Les règles qui génèrent des `SuspiciousTool` résultats incluent `ToolName` et `ToolCategory`.

Ressource

Chaque résultat couvre une ressource unique, telle qu'une instance, une tâche ou un conteneur. Pour plus d'informations sur la façon dont GuardDuty les signaux de groupe sont regroupés, consultez [Trouver une agrégation](#).

Détails de l'utilisateur de base de données (DB) RDS

Note

Cette section s'applique aux résultats obtenus lorsque vous activez la fonctionnalité de protection RDS dans GuardDuty. Pour plus d'informations, consultez [GuardDuty Protection RDS](#).

La GuardDuty découverte fournit les informations suivantes relatives à l'utilisateur et à l'authentification de la base de données potentiellement compromise :

- Utilisateur : nom d'utilisateur utilisé pour effectuer la tentative de connexion anormale.
- Application : nom de l'application servant à effectuer la tentative de connexion anormale.
- Base de données : nom de l'instance de base de données impliquée dans la tentative de connexion anormale.
- SSL : version du protocole SSL (Secure Socket Layer) utilisée pour le réseau.
- Méthode d'authentification : méthode d'authentification utilisée par l'utilisateur impliqué dans le résultat.

Pour plus d'informations sur la ressource potentiellement compromise, consultez [Ressource](#).

Surveillance d'exécution : détails des résultats

Note

Ces informations ne peuvent être disponibles que GuardDuty si l'un des [GuardDuty Types de recherche liés à la surveillance du temps](#).

Cette section contient les détails de l'exécution, tels que les détails du processus et tout contexte requis. Les détails du processus décrivent les informations relatives au processus observé, et le contexte d'exécution décrit toute information supplémentaire concernant l'activité potentiellement suspecte.

Détails du processus

- Nom : nom du processus.
- Chemin exécutable : chemin absolu du fichier exécutable du processus.
- Exécutable SHA-256 — Le SHA256 hachage de l'exécutable du processus.
- PID de l'espace de noms : ID du processus dans un espace de noms PID secondaire différent de l'espace de noms PID au niveau de l'hôte. Pour les processus se trouvant à l'intérieur d'un conteneur, il s'agit de l'ID de processus observé à l'intérieur du conteneur.
- Répertoire de travail actuel : répertoire de travail actuel du processus.
- ID de processus : ID attribué au processus par le système d'exploitation.
- startTime : heure à laquelle le processus a démarré. Ce champ est au format de chaîne de date UTC (2023-03-22T19:37:20.168Z).
- UUID — L'identifiant unique attribué au processus par GuardDuty
- UUID parent : identifiant unique du processus parent. Cet identifiant est attribué au processus parent par GuardDuty.
- Utilisateur : utilisateur qui a exécuté le processus.
- ID utilisateur : ID de l'utilisateur qui a exécuté le processus.
- ID utilisateur effectif : ID de l'utilisateur effectif du processus au moment de l'événement.
- Lignée : informations sur les ancêtres du processus.
 - ID de processus : ID attribué au processus par le système d'exploitation.
 - UUID — L'identifiant unique attribué au processus par GuardDuty
 - Chemin exécutable : chemin absolu du fichier exécutable du processus.
 - ID utilisateur effectif : ID de l'utilisateur effectif du processus au moment de l'événement.
 - UUID parent : identifiant unique du processus parent. Cet identifiant est attribué au processus parent par GuardDuty.
 - Heure de début : heure à laquelle le processus a démarré.

- PID de l'espace de noms : ID du processus dans un espace de noms PID secondaire différent de l'espace de noms PID au niveau de l'hôte. Pour les processus se trouvant à l'intérieur d'un conteneur, il s'agit de l'ID de processus observé à l'intérieur du conteneur.
- ID utilisateur : ID de l'utilisateur qui a exécuté le processus.
- Nom : nom du processus.

Contexte d'exécution

Parmi les champs suivants, un résultat généré peut inclure uniquement les champs correspondant au type de résultat.

- Source de montage : chemin sur l'hôte monté par le conteneur.
- Cible de montage : chemin du conteneur mappé au répertoire hôte.
- Type de système de fichiers : représente le type du système de fichiers monté.
- Indicateurs : représente les options qui contrôlent le comportement de l'événement impliqué dans ce résultat.
- Processus de modification : informations sur le processus qui a créé ou modifié un fichier binaire, un script ou une bibliothèque dans un conteneur lors de l'exécution.
- Modifié à : horodatage auquel le processus a créé ou modifié un binaire, un script ou une bibliothèque dans un conteneur au moment de l'exécution. Ce champ est au format de chaîne de date UTC (2023-03-22T19:37:20.168Z).
- Chemin de la bibliothèque : chemin d'accès à la nouvelle bibliothèque chargée.
- Valeur de préchargement LD : valeur de la variable d'environnement LD_PRELOAD.
- Chemin du socket : chemin d'accès au socket Docker auquel l'utilisateur a accédé.
- Chemin d'accès au binaire Runc : chemin d'accès au binaire runc.
- Chemin d'accès à l'agent de version : chemin d'accès au fichier de l'agent de version cgroup.
- Exemple de ligne de commande : exemple de ligne de commande impliquée dans l'activité potentiellement suspecte.
- Catégorie d'outil : catégorie à laquelle appartient l'outil. Voici quelques exemples : Backdoor Tool, Pentest Tool, Network Scanner et Network Sniffer.
- Nom de l'outil : nom de l'outil potentiellement suspect.
- Opération de fichier : type d'opération de fichier qui a déclenché la recherche, telle que Write, Delete, Rename, Link ou Symlink.

- Chemin du fichier : chemin du fichier sensible qui a été modifié. La modification inclut les opérations d'écriture, de suppression, de renommage, de liaison ou de lien symbolique.
- Chemins de fichiers associés : tous les chemins de fichiers modifiés par le même processus qui a déclenché la recherche, dans la limite de 25 chemins.
- Chemin du script : chemin d'accès au script exécuté qui a généré le résultat.
- Chemin du fichier de menaces : chemin suspect pour lequel les informations relatives aux menaces ont été trouvées.
- Nom du service : nom du service de sécurité qui a été désactivé.
- Nom du module : nom du module chargé dans le noyau.
- Module SHA256 — Le hachage SHA256 du module.
- Chemin du fichier du module : chemin d'accès au module chargé dans le noyau.

Détails de l'analyse des volumes EBS

Note

Cette section s'applique aux résultats lorsque vous activez l'analyse des GuardDuty-initiated programmes malveillants [Protection contre les logiciels malveillants pour EC2](#).

L'analyse des volumes EBS fournit des informations détaillées sur le volume EBS attaché à l'instance EC2 ou à la charge de travail du conteneur potentiellement compromise.

- ID de numérisation : identifiant de l'analyse des logiciels malveillants.
- Analyse démarrée à : date et heure du début de l'analyse des logiciels malveillants.
- Analyse terminée à : date et heure de fin de l'analyse des logiciels malveillants.
- ID de recherche du déclencheur : ID de recherche du GuardDuty résultat à l'origine de cette analyse des logiciels malveillants.
- Sources — Les valeurs potentielles sont Bitdefender et Amazon.

Pour plus d'informations sur le moteur d'analyse utilisé pour détecter les programmes malveillants, consultez [GuardDuty moteur d'analyse pour la détection des malwares](#).

- Détections d'analyse : vue complète des détails et des résultats de chaque analyse des logiciels malveillants.

- Nombre d'éléments analysés : nombre total de fichiers numérisés. Fournit des détails tels que `totalGb`, `files` et `volumes`.
- Nombre d'éléments de menaces détectées : nombre total de files malveillants détectés lors de l'analyse.
- Informations sur les menaces les plus graves : informations sur la menace la plus grave détectée lors de l'analyse et sur le nombre de fichiers malveillants. Fournit des détails tels que `severity`, `threatName` et `count`.
- Menaces détectées par nom : élément du conteneur regroupant les menaces de tous niveaux de gravité. Fournit des détails tels que `itemCount`, `uniqueThreatNameCount`, `shortened` et `threatNames`.

Protection contre les logiciels malveillants pour la recherche de détails dans EC2

Note

Cette section s'applique aux résultats lorsque vous activez l'analyse des GuardDuty-initiated programmes malveillants [Protection contre les logiciels malveillants pour EC2](#).

Lorsque l'analyse Malware Protection for EC2 détecte un logiciel malveillant, vous pouvez consulter les détails de l'analyse en sélectionnant le résultat correspondant sur la page Résultats de la <https://console.aws.amazon.com/guardduty/console>. La gravité de votre détection de Malware Protection for EC2 dépend de la gravité de la GuardDuty découverte.

Les informations suivantes sont disponibles dans la section Menaces détectées du panneau de détails.

- Nom : nom de la menace, obtenu en groupant les fichiers par détection.
- Gravité : gravité de la menace détectée.
- Hash — Le nom SHA-256 du fichier.
- Chemin d'accès du fichier : emplacement du fichier malveillant dans le volume EBS.
- Nom du fichier : nom du fichier dans lequel la menace a été détectée.
- ARN du volume : ARN des volumes EBS analysés.

Les informations suivantes sont disponibles dans la section Détails de l'analyse des logiciels malveillants du panneau des détails.

- ID de numérisation : ID de numérisation des logiciels malveillants.
- Analyse démarrée à : date et heure du début de l'analyse.
- Analyse terminée à : date et heure de fin de l'analyse.
- Fichiers analysés : nombre total de fichiers et de répertoires numérisés.
- Nombre total de Go numérisés : quantité de stockage analysée au cours du processus.
- ID de recherche du déclencheur : ID de recherche du GuardDuty résultat à l'origine de cette analyse des logiciels malveillants.
- Les informations suivantes sont disponibles dans la section Détails de volume du panneau des détails.
 - ARN du volume : Amazon Resource Name (ARN) du volume.
 - SnapshotARN : ARN de l'instantané du volume EBS.
 - État : état de l'analyse du volume, tel que Running, Skipped et Completed.
 - Type de chiffrement : type de chiffrement utilisé pour chiffrer le volume. Par exemple : CCMK.
 - Nom de l'appareil : nom de l'appareil. Par exemple : /dev/xvda.

Informations sur la recherche effectuée par la protection contre les logiciels malveillants pour S3

Les informations suivantes relatives à l'analyse des programmes malveillants sont disponibles lorsque vous activez à la fois GuardDuty la protection contre les programmes malveillants pour S3 dans votre Compte AWS :

- Menaces : liste des menaces détectées lors de l'analyse des logiciels malveillants.

Menaces potentielles multiples dans les fichiers d'archive

Si vous avez un fichier d'archive contenant potentiellement plusieurs menaces, Malware Protection for S3 ne signale que la première menace détectée. Après cela, l'état du scan est marqué comme terminé. GuardDuty génère le type de recherche associé et envoie également EventBridge les événements qu'il génère. Pour plus d'informations sur la surveillance des objets analysés par Amazon S3 à l'aide EventBridge des événements,

consultez l'exemple de schéma de notification pour THREATS_FOUND dans. [Résultat de l'analyse d'objets S3](#)

- Chemin de l'élément : liste des chemins d'éléments imbriqués et des détails de hachage de l'objet S3 scanné.
- Chemin de l'élément imbriqué : chemin de l'élément de l'objet S3 scanné où la menace a été détectée.

La valeur de ce champ n'est disponible que si l'objet de niveau supérieur est une archive et si une menace est détectée dans une archive.

- Hachage : hachage de la menace détectée dans cette constatation.

Note

Dans les cas où le hachage ne peut pas être calculé, le résultat de l'analyse est toujours fourni et la valeur SHA-256 de hachage par défaut est une chaîne vide ().
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

- Sources — Les valeurs potentielles sont Bitdefender et Amazon.

Pour plus d'informations sur le moteur d'analyse utilisé pour détecter les programmes malveillants, consultez [GuardDuty moteur d'analyse pour la détection des malwares](#).

Action

L'action d'un résultat donne des détails sur le type d'activité qui a déclenché le résultat. Les informations disponibles varient selon le type d'action.

Type d'action : type d'activité du résultat. Cette valeur peut être NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST ou RDS_LOGIN_ATTEMPT. AWS_API_CALL Les informations disponibles varient selon le type d'action :

- NETWORK_CONNECTION : indique qu'un trafic réseau a été échangé entre l'instance EC2 identifiée et l'hôte distant. Ce type d'action contient les informations supplémentaires suivantes :
 - Direction de connexion : direction de connexion réseau observée lors de l'activité qui a incité GuardDuty à générer le résultat. Il peut s'agir de l'une des valeurs suivantes :

- **INBOUND** : indique qu'un hôte distant a initié une connexion à un port local sur l'instance EC2 identifiée dans votre compte.
- **OUTBOUND** : indique que l'instance EC2 identifiée a initié une connexion à un hôte distant.
- **INCONNU** — Indique qu'il n'a pas été possible de déterminer le sens de la connexion.
- **Protocole** : protocole de connexion réseau observé dans l'activité qui a incité GuardDuty à générer le résultat.
- **IP locale** : adresse IP source d'origine du trafic ayant déclenché le résultat. Cette information permet de faire la distinction entre l'adresse IP d'une couche intermédiaire via laquelle les flux transitent et l'adresse IP source d'origine du trafic qui a déclenché la recherche. Par exemple, l'adresse IP d'un pod EKS par opposition à l'adresse IP de l'instance sur laquelle le pod EKS s'exécute.
- **Bloqué** : indique si le port cible est bloqué.
- **PORT_PROBE** : indique qu'un hôte distant a fait l'objet d'une identification de l'instance EC2 sur plusieurs ports ouverts. Ce type d'action contient les informations supplémentaires suivantes :
 - **IP locale** : adresse IP source d'origine du trafic ayant déclenché le résultat. Cette information permet de faire la distinction entre l'adresse IP d'une couche intermédiaire via laquelle les flux transitent et l'adresse IP source d'origine du trafic qui a déclenché la recherche. Par exemple, l'adresse IP d'un pod EKS par opposition à l'adresse IP de l'instance sur laquelle le pod EKS s'exécute.
 - **Bloqué** : indique si le port cible est bloqué.
- **DNS_REQUEST** : indique que l'instance EC2 identifiée a interrogé un nom de domaine. Ce type d'action contient les informations supplémentaires suivantes :
 - **Protocole** : protocole de connexion réseau observé dans l'activité qui a incité GuardDuty à générer le résultat.
 - **Bloqué** : indique si le port cible est bloqué.
- **AWS_API_CALL** — Indique qu'une AWS API a été invoquée. Ce type d'action contient les informations supplémentaires suivantes :
 - **API** : nom de l'opération d'API qui a été invoquée et donc invitée GuardDuty à générer ce résultat.

 Note

Ces opérations peuvent également inclure des événements non API capturés par AWS CloudTrail. Pour plus d'informations, consultez la section [Non-API Événements capturés par CloudTrail](#).

- **Agent utilisateur** : agent utilisateur à l'origine de la demande d'API. Cette valeur vous indique si l'appel a été effectué à partir du Console de gestion AWS, d'un AWS service, AWS des SDK ou du AWS CLI.
- **CODE D'ERREUR** : si le résultat a été déclenché par l'échec d'un appel d'API, le code d'erreur correspondant à cet appel est affiché.
- **Nom du service** : nom DNS du service qui a tenté d'effectuer l'appel d'API ayant déclenché le résultat.
- **RDS_LOGIN_ATTEMPT** : indique qu'une tentative de connexion a été effectuée à la base de données potentiellement compromise à partir d'une adresse IP distante.
- **Adresse IP** : adresse IP distante utilisée pour effectuer la tentative de connexion potentiellement suspecte.

Acteur ou cible

Un résultat a une section Acteur si le rôle de la ressource était TARGET. Cela indique que votre ressource a été ciblée par une activité suspecte, et la section Acteur contient des détails sur l'entité qui a ciblé votre ressource.

Un résultat a une section Cible si le rôle de la ressource était ACTOR. Cela indique que votre ressource a été impliquée dans une activité suspecte contre un hôte distant, et cette section contiendra des informations sur l'IP ou le domaine ciblé par votre ressource.

Les informations disponibles dans la section Acteur ou Cible peuvent inclure les éléments suivants :

- **Affilié** : indique si le AWS compte de l'appelant de l'API distant est lié à votre GuardDuty environnement. Si cette valeur est `true`, l'appelant de l'API est affilié à votre compte d'une manière ou d'une autre, tandis que si cette valeur est `false`, l'appelant de l'API vient de l'extérieur de votre environnement.
- **ID de compte distant** : ID de compte propriétaire de l'adresse IP sortante utilisée pour accéder à la ressource sur le réseau final.

- Adresse IP : adresse IP impliquée dans l'activité qui a incité GuardDuty à générer le résultat.
- Emplacement : informations de localisation de l'adresse IP impliquée dans l'activité GuardDuty à l'origine de la recherche.
- Organisation — Informations relatives à l'adresse IP associée à l'activité à l'origine de la constatation auprès de l'organisation du GuardDuty fournisseur de services Internet.
- Port : numéro de port impliqué dans l'activité GuardDuty à l'origine de la recherche.
- Domaine : domaine impliqué dans l'activité qui a incité GuardDuty à générer le résultat.
- Domaine avec suffixe : domaine de deuxième et de premier niveau impliqué dans une activité susceptible d'inciter GuardDuty à générer le résultat. Pour obtenir la liste des domaines de premier et de deuxième niveau, consultez la liste des [suffixes publics](#).

Détails de géolocalisation

GuardDuty détermine l'emplacement et le réseau des demandes à l'aide de bases de MaxMind données GeoIP. MaxMind fait état d'une très grande précision de ses données au niveau du pays, bien que la précision varie en fonction de facteurs tels que le pays et le type d'adresse IP.

Pour plus d'informations MaxMind, consultez la section [Géolocalisation MaxMind IP](#). Si vous pensez que l'une des données GeoIP est incorrecte, envoyez une demande de correction à MaxMind at [MaxMindCorrect GeoIP2](#) Data.

Informations supplémentaires

Tous les résultats ont une section Informations supplémentaires incluant les informations suivantes :

- Nom de la liste de menaces : nom de la liste de menaces qui inclut l'adresse IP ou le nom de domaine impliqué dans l'activité GuardDuty à l'origine de la découverte.
- Exemple : une valeur vraie ou fausse qui indique s'il s'agit d'un exemple de résultat.
- Archivé : une valeur vraie ou fausse qui indique si ce résultat a été archivé.
- Inhabituelle : détails d'une activité qui n'a pas été observée historiquement. Cela peut inclure tout utilisateur, emplacement, moment, compartiment, comportement de connexion ou organisation ASN inhabituel (non observé précédemment).
- Protocole inhabituel : protocole de connexion réseau impliqué dans l'activité GuardDuty à l'origine du résultat.
- Détails de l'agent : détails sur l'agent de sécurité actuellement déployé sur le cluster EKS de votre Compte AWS. Cela ne s'applique qu'aux types de résultat de la surveillance d'exécution EKS.

- Version de l'agent : version de l'agent GuardDuty de sécurité.
- ID de l'agent : identifiant unique de l'agent GuardDuty de sécurité.

Preuve

Les résultats basés sur les renseignements sur les menaces comportent une section Preuve qui comprend les informations suivantes :

- Informations détaillées sur les menaces : nom de la liste des menaces sur laquelle Threat name figure la menace reconnue.
- Nom de la menace : nom de la famille de logiciels malveillants ou autre identifiant associé à la menace.
- Fichier de menace SHA256 — SHA256 du fichier qui a généré le résultat.

Comportement anormal

Les types de résultats qui se terminent par AnomalousBehavior indiquent que le résultat a été généré par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle de ML évalue toutes les demandes d'API adressées à votre compte et identifie les événements anormaux associés aux tactiques utilisées par les adversaires. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée.

Vous trouverez des informations sur les facteurs de la demande d'API inhabituels pour l'identité de l' CloudTrail utilisateur qui a invoqué la demande dans les détails de la recherche. Les identités sont définies par l'[élément CloudTrail UserIdentity](#), et les valeurs possibles sont les suivantes :Root,IAMUser,, AssumedRole FederatedUserAWSAccount, ou. AWSService

Outre les détails disponibles pour tous les GuardDuty résultats associés à l'activité de l'API, AnomalousBehaviorles résultats contiennent des informations supplémentaires qui sont décrites dans la section suivante. Ces détails peuvent être consultés dans la console et sont également disponibles dans le fichier JSON du résultat.

- API anormales : liste des demandes d'API invoquées par l'identité de l'utilisateur à proximité de la demande d'API principale associée au résultat. Ce volet détaille plus en détail l'événement d'API de la manière suivante.

- La première API répertoriée est l'API principale, qui est la demande d'API associée à l'activité observée présentant le plus haut risque. Il s'agit de l'API qui a déclenché le résultat et qui est corrélée à la phase d'attaque du type de résultat. Il s'agit également de l'API qui est détaillée dans la section Action de la console et dans le fichier JSON du résultat.
- Toutes les autres API répertoriées sont des API anormales supplémentaires provenant de l'identité utilisateur répertoriée observée à proximité de l'API principale. S'il n'y a qu'une seule API dans la liste, le modèle de ML n'a identifié aucune demande d'API supplémentaire provenant de cette identité d'utilisateur comme anormale.
- La liste des API est divisée selon qu'une API a été appelée avec succès ou non, ce qui signifie qu'une réponse d'erreur a été reçue. Le type de réponse d'erreur reçue est indiqué au-dessus de chaque API appelée sans succès. Les types de réponse d'erreur possibles sont les suivants : `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` et `operation not permitted`.
- Les API sont classées en fonction du service qui leur est associé.
- Pour plus de contexte, choisissez API historiques pour afficher les détails des principales API, jusqu'à un maximum de 20, généralement visibles à la fois pour l'identité de l'utilisateur et pour tous les utilisateurs du compte. Les API sont marquées comme Rare (moins d'une fois par mois), Peu fréquent (quelques fois par mois) ou Fréquent (quotidien ou hebdomadaire), selon la fréquence à laquelle elles sont utilisées dans votre compte.
- Comportement inhabituel (compte) : cette section fournit des informations supplémentaires sur le comportement profilé de votre compte.

Comportement profilé

GuardDuty se renseigne en permanence sur les activités de votre compte en fonction des événements survenus. Ces activités et leur fréquence observée sont connues sous le nom de comportement profilé.

Les informations suivies dans ce panneau incluent :

- Organisation ASN : organisation ASN (Autonomous System Number) à partir de laquelle l'appel d'API anormal a été effectué.
- Nom d'utilisateur : nom de l'utilisateur qui a effectué l'appel d'API anormal.

- **Agent utilisateur** : agent utilisateur utilisé pour effectuer l'appel d'API anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
- **Type d'utilisateur** : type d'utilisateur qui a effectué l'appel d'API anormal. Les valeurs possibles sont `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.
- **Compartiment** : nom du compartiment S3 auquel on a accédé.
- **Comportement inhabituel (identité de l'utilisateur)** : cette section fournit des détails supplémentaires sur le comportement profilé de l'identité de l'utilisateur impliqué dans le résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a jamais vu cette identité d'utilisateur effectuer cet appel d'API de cette manière au cours de la période de formation. Les informations supplémentaires suivantes concernant l'identité de l'utilisateur sont disponibles :
 - **Organisation ASN** : organisation ASN à partir de laquelle l'appel d'API anormal a été effectué.
 - **Agent utilisateur** : agent utilisateur utilisé pour effectuer l'appel d'API anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
 - **Compartiment** : nom du compartiment S3 auquel on a accédé.
- **Comportement inhabituel (compartiment)** : cette section fournit des informations supplémentaires sur le comportement profilé du compartiment S3 associé au résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle de GuardDuty machine learning n'a jamais vu d'appels d'API effectués de cette manière vers ce bucket au cours de la période de formation. Les informations suivies dans cette section incluent :
 - **Organisation ASN** : organisation ASN à partir de laquelle l'appel d'API anormal a été effectué.
 - **Nom d'utilisateur** : nom de l'utilisateur qui a effectué l'appel d'API anormal.
 - **Agent utilisateur** : agent utilisateur utilisé pour effectuer l'appel d'API anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
 - **Type d'utilisateur** : type d'utilisateur qui a effectué l'appel d'API anormal. Les valeurs possibles sont `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.

Note

Pour plus de détails sur les comportements historiques, choisissez Comportement historique dans la section Comportement inhabituel (compte), ID utilisateur ou Compartiment pour afficher les détails du comportement attendu dans votre compte pour chacune des catégories suivantes : Rare (moins d'une fois par mois), Peu fréquent

(quelques fois par mois) ou Fréquent (quotidien ou hebdomadaire), selon la fréquence à laquelle ils sont utilisés dans votre compte.

- **Comportement inhabituel (base de données) :** cette section fournit des informations supplémentaires sur le comportement profilé de l'instance de base de données associée au résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a jamais connu de tentative de connexion de cette manière à cette instance de base de données au cours de la période de formation. Les informations suivies pour cette section dans le panneau de résultat incluent :
 - **Nom d'utilisateur :** nom d'utilisateur utilisé pour effectuer la tentative de connexion anormale.
 - **Organisation ASN :** organisation ASN à partir de laquelle la tentative de connexion anormale a été effectuée.
 - **Nom de l'application :** nom de l'application servant à effectuer la tentative de connexion anormale.
 - **Nom de la base de données :** nom de l'instance de base de données impliquée dans la tentative de connexion anormale.

La section Comportement historique fournit plus de contexte sur les noms d'utilisateur, les organisations ASN, les noms d'applications et les noms de base de données précédemment observés pour la base de données associée. Chaque valeur unique est associée à un nombre représentant le nombre de fois qu'elle a été observée lors d'un événement de connexion qui a abouti.

- **Comportement inhabituel (cluster Kubernetes de compte, espace de noms Kubernetes et nom d'utilisateur Kubernetes) :** cette section fournit des informations supplémentaires sur le comportement profilé du cluster Kubernetes et de l'espace de noms associé au résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a pas précédemment observé ce compte, ce cluster, cet espace de noms ou ce nom d'utilisateur de cette manière. Les informations suivies pour cette section dans le panneau de résultat incluent :
 - **Nom d'utilisateur :** utilisateur qui a appelé l'API Kubernetes associée au résultat.
 - **Nom d'utilisateur usurpé :** l'utilisateur usurpé par `username`.
 - **Espace de noms :** espace de noms Kubernetes au sein du cluster Amazon EKS où l'action s'est produite.
 - **Agent utilisateur :** agent utilisateur associé à l'appel d'API Kubernetes. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `kubectl`.
 - **API :** l'API Kubernetes appelée par `username` au sein du cluster Amazon EKS.

- Informations ASN : informations ASN, telles que l'organisation et le fournisseur de services Internet, associées à l'adresse IP de l'utilisateur à l'origine de cet appel.
- Jour de la semaine : jour de la semaine où l'appel d'API Kubernetes a été effectué.
- Autorisation — Le verbe et la ressource Kubernetes dont l'accès est vérifié pour indiquer s'ils username peuvent ou non utiliser l'API Kubernetes.
- Nom du compte de service : compte de service associé à la charge de travail Kubernetes qui fournit une identité à la charge de travail.
- Registre : registre de conteneurs associé à l'image de conteneur déployée dans le workload Kubernetes.
- Image : image du conteneur, sans les balises ni le résumé associés, déployée dans le workload Kubernetes.
- Config du préfixe d'image : préfixe d'image pour lequel la configuration de sécurité du conteneur et de la charge de travail est activée `privileged`, par exemple `hostNetwork` ou pour le conteneur utilisant l'image.
- Nom du sujet — Les sujets, tels que `usergroup`, ou `serviceName` qui sont liés à un rôle de référence dans un `RoleBinding` ou `ClusterRoleBinding`.
- Nom du rôle : nom du rôle impliqué dans la création ou la modification des rôles ou de `roleBindingAPI`.

Anomalies basées sur le volume S3

Cette section détaille les informations contextuelles relatives aux anomalies basées sur le volume S3. Le résultat basé sur le volume ([Exfiltration:S3/AnomalousBehavior](#)) surveille le nombre inhabituel d'appels d'API S3 adressés par les utilisateurs aux compartiments S3, ce qui indique une exfiltration potentielle de données. Les appels d'API S3 suivants sont surveillés pour détecter les anomalies basées sur le volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Les métriques suivantes aideront à établir une référence du comportement habituel lorsqu'une entité IAM accède à un compartiment S3. Pour détecter l'exfiltration de données, le résultat de détection d'anomalies basées sur le volume évalue toutes les activités par rapport à la

référence comportementale habituelle. Choisissez Comportement historique dans les sections Comportement inhabituel (identité utilisateur), Volume observé (identité utilisateur) et Volume observé (compartiment) pour afficher les métriques suivantes, respectivement.

- Nombre d'appels d'API `s3-api-name` invoqués par l'utilisateur IAM ou le rôle IAM (selon celui qui a été émis) associés au compartiment S3 concerné au cours des dernières 24 heures.
- Nombre d'appels d'API `s3-api-name` invoqués par l'utilisateur IAM ou le rôle IAM (selon celui qui a été émis) associés à tous les compartiments S3 au cours des dernières 24 heures.
- Nombre d'appels d'API `s3-api-name` entre tous les utilisateurs IAM ou rôles IAM (selon celui qui a été émis) associés au compartiment S3 concerné au cours des dernières 24 heures.

Anomalies basées sur l'activité de connexion RDS

Cette section détaille le nombre de tentatives de connexion effectuées par l'acteur inhabituel et est regroupée en fonction du résultat des tentatives de connexion. Les [Types de résultat de la protection RDS](#) identifient les comportements anormaux en surveillant les événements de connexion pour détecter les modèles inhabituels de `successfulLoginCount`, `failedLoginCount` et `incompleteConnectionCount`.

- réussi LoginCount — Ce compteur représente la somme des connexions réussies (combinaison correcte d'attributs de connexion) établies avec l'instance de base de données par l'acteur inhabituel. Les attributs de connexion incluent le nom d'utilisateur, le mot de passe et le nom de la base de données.
- échec LoginCount — Ce compteur représente la somme des tentatives de connexion infructueuses (infructueuses) effectuées pour établir une connexion à l'instance de base de données. Il indique qu'un ou plusieurs attributs de la combinaison de connexion, tels que le nom d'utilisateur, le mot de passe ou le nom de base de données, étaient incorrects.
- incomplet ConnectionCount — Ce compteur représente le nombre de tentatives de connexion qui ne peuvent être classées comme réussies ou échouées. Ces connexions sont fermées avant que la base de données ne fournisse une réponse. Par exemple, l'analyse des ports lorsque le port de base de données est connecté, mais qu'aucune information n'est envoyée à la base de données, ou lorsque la connexion a été interrompue avant la fin de la connexion lors d'une tentative réussie ou infructueuse.

Anomalies liées à l'activité des données RDS

Cette section décrit les activités anormales liées aux données, telles qu'un acteur lisant beaucoup plus de lignes ou supprimant ou supprimant plus de données que ce qui est normal pour cette base de données et cet utilisateur. Ils [Types de résultat de la protection RDS](#) identifient les comportements anormaux en surveillant l'activité de la base de données pour détecter des modèles inhabituels dans le nombre de lignes lues ou supprimées et dans les instructions de suppression.

- `selectedRowset selectStatement` — Ces compteurs représentent le nombre de lignes renvoyées par les SELECT instructions et le nombre d'SELECTinstructions observées dans le cadre de l'activité associée au résultat.
- `deletedRowset deleteStatement` — Ces compteurs représentent le nombre de lignes supprimées par les DELETE instructions et le nombre d'DELETEinstructions observées dans l'activité associée au résultat.
- `dropStatement`— Ce compteur représente le nombre d'opérations destructrices, telles que DROP ouTRUNCATE, qui peuvent supprimer des objets de base de données ou des données dans le cadre de l'activité associée à la découverte.

GuardDuty pourrait collecter des données télémétriques supplémentaires, telles que de nouveaux compteurs, à l'avenir afin d'améliorer l'efficacité des résultats d'activité des données et d'introduire de nouvelles détections de menaces par RDS Protection.

GuardDuty recherche d'agrégation

GuardDuty met à jour les résultats générés de manière dynamique. Si une nouvelle activité liée au même problème de sécurité est GuardDuty détectée, au lieu de créer une nouvelle découverte, la découverte d'origine GuardDuty sera mise à jour avec les informations les plus récentes. Ce comportement vous permet d'identifier tout problème persistant, sans avoir à consulter plusieurs rapports similaires, et réduit le volume global de résultats concernant les problèmes de sécurité connus.

Par exemple, pour la UnauthorizedAccess:EC2/SSHBruteForce recherche, plusieurs tentatives d'accès à votre instance seront agrégées sous le même identifiant de recherche, ce qui augmentera le nombre de tentatives dans les détails de la découverte. Cela est dû au fait que ce résultat représente un même problème de sécurité lié à l'instance indiquant que le port SSH de l'instance n'est pas correctement sécurisé contre ce type d'activité. Toutefois, si GuardDuty détecte une activité d'accès SSH ciblant une nouvelle instance dans votre environnement, il crée un nouveau résultat

avec un ID de résultat unique pour vous alerter sur le fait qu'il existe un problème de sécurité lié à la nouvelle ressource.

Lorsqu'un résultat est agrégé, il est mis à jour avec les informations relatives à la dernière occurrence de cette activité. Dans l'exemple ci-dessus, cela signifie que si votre instance est la cible d'une tentative d'attaque en force de la part d'un nouvel acteur, les détails du résultat seront mis à jour pour refléter l'adresse IP distante de la source la plus récente et les informations plus anciennes seront remplacées. Des informations complètes sur les tentatives d'activité individuelles seront toujours disponibles dans vos CloudTrail journaux ou les journaux de flux VPC.

Les critères qui permettent GuardDuty de générer un nouveau résultat au lieu d'agréger un résultat existant dépendent du type de résultat. Les critères d'agrégation pour chaque type de découverte sont déterminés par nos ingénieurs de sécurité afin de fournir un aperçu des différents problèmes de sécurité liés à votre compte.

Lorsque vous GuardDuty générez un type de recherche de séquence d'attaque dans votre compte, le résultat ne sera agrégé que lorsque vous GuardDuty identifierez les signaux similaires dans la même séquence sur votre compte. Sinon, une autre séquence d'attaque GuardDuty sera générée.

Gérer les GuardDuty résultats d'Amazon

GuardDuty propose plusieurs fonctionnalités importantes pour vous aider à trier, stocker et gérer vos résultats. Ces fonctionnalités vous aideront à adapter les résultats à votre environnement spécifique, à réduire le bruit généré par les résultats de faible valeur et à vous concentrer sur les menaces qui pèsent sur votre AWS environnement spécifique. Consultez les rubriques de cette page pour comprendre comment utiliser ces fonctionnalités afin d'accroître la valeur des résultats de sécurité dans votre environnement.

Rubriques :

[Tableau de bord récapitulatif sur Amazon GuardDuty](#)

Découvrez les composants du tableau de bord récapitulatif disponible dans la GuardDuty console.

[Filtrer les résultats dans GuardDuty](#)

Découvrez comment filtrer les GuardDuty résultats en fonction des critères que vous spécifiez.

[Règles de suppression dans GuardDuty](#)

Découvrez comment filtrer automatiquement les résultats qui vous sont GuardDuty signalés par le biais de règles de suppression. Les règles de suppression archivent automatiquement les résultats en fonction de filtres.

[Personnalisation de la détection des menaces à l'aide de listes d'entités et de listes d'adresses IP](#)

Personnalisez le périmètre GuardDuty de surveillance à l'aide de listes d'adresses IP et de listes de menaces basées sur des adresses IP routables publiquement. Les listes d'adresses IP fiables empêchent de générer des résultats non liés au DNS à partir d'adresses IP que vous considérez comme fiables, tandis que les listes d'informations sur les menaces vous alerteront GuardDuty en cas d'activité provenant d'adresses IP définies par l'utilisateur.

[Exportation des résultats générés vers Amazon S3](#)

Exportez les résultats générés vers un compartiment Amazon S3 afin de pouvoir conserver les dossiers au-delà de la période de conservation de 90 jours prévue GuardDuty pour. Utilisez ces données historiques pour suivre les activités suspectes potentielles sur votre compte et évaluer si les mesures correctives recommandées ont été efficaces.

Traitement des GuardDuty résultats avec Amazon EventBridge

Configurez des notifications automatiques pour les GuardDuty résultats obtenus par le biais d' EventBridge événements Amazon. Vous pouvez également automatiser d'autres tâches EventBridge pour vous aider à répondre aux résultats.

Comprendre CloudWatch les journaux et les raisons pour lesquelles des ressources sont ignorées lors de l'analyse Malware Protection for EC2

Découvrez comment auditer les CloudWatch journaux de protection contre les GuardDuty programmes malveillants pour EC2 et quelles sont les raisons pour lesquelles votre instance Amazon EC2 ou vos volumes Amazon EBS concernés peuvent avoir été ignorés pendant le processus de numérisation.

Signalement des faux positifs dans Malware Protection for EC2

Découvrez comment signaler les détections potentielles de fausses menaces positives dans Malware Protection for EC2.

Signaler le résultat de l'analyse d'un objet S3 comme faux positif dans Malware Protection for S3

Découvrez comment signaler les détections potentielles de fausses menaces positives dans Malware Protection for S3.

Signalement de faux positifs dans Malware Protection for Backup

Découvrez comment signaler les détections potentielles de faux positifs dans Malware Protection for Backup.

Tableau de bord récapitulatif sur Amazon GuardDuty

Le tableau de bord GuardDuty récapitulatif fournit une vue agrégée des GuardDuty résultats générés Compte AWS dans votre compte actuel Région AWS.

Si vous utilisez un compte GuardDuty administrateur, le tableau de bord fournit des statistiques et des données agrégées pour votre compte et les comptes des membres de votre organisation.

Affichage du tableau de bord récapitulatif

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.

GuardDuty affiche le tableau de bord récapitulatif par défaut lorsque vous ouvrez la console.

2. Sur la page Résumé, choisissez la région souhaitée dans le sélecteur Région AWS de région situé dans le coin supérieur droit de la console.
3. Dans le menu de sélection de la plage de dates, choisissez la plage de dates pour laquelle vous souhaitez afficher le résumé. Par défaut, le tableau de bord affiche les données du jour actuel, Today.

 Note

Si aucun résultat n'a été généré pendant la période sélectionnée, le tableau de bord ne contiendra aucune donnée à afficher. Vous pouvez actualiser le tableau de bord ou ajuster la plage de dates.

Rubriques

- [Présentation de](#)
- [Résultats](#)
- [Types de résultat les plus courants](#)
- [Résultats par gravité](#)
- [Comptes contenant le plus de résultats](#)
- [Ressources contenant des résultats](#)
- [Résultats les moins fréquents](#)
- [Couverture des plans de protection](#)

Présentation de

Cette section fournit les données suivantes :

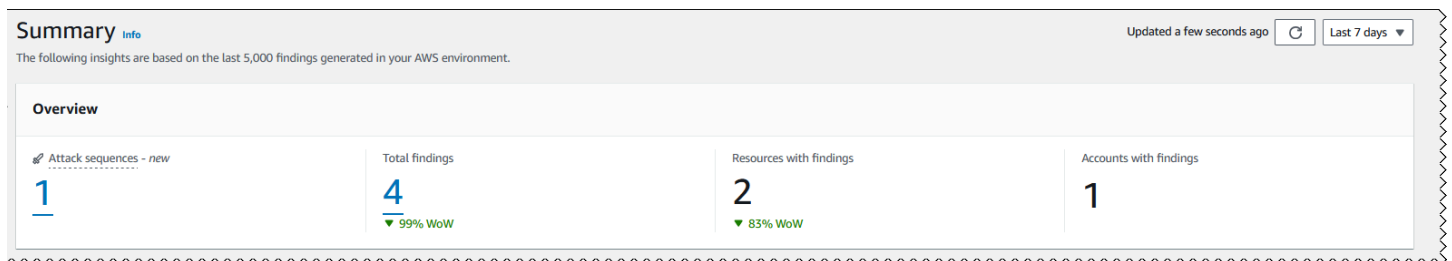
- Séquences d'attaque : indique le nombre de séquences d' GuardDuty attaques détectées sur votre compte dans la région actuelle.

GuardDuty détecte les attaques potentielles en plusieurs étapes sur votre compte. Vous pouvez sélectionner le numéro sous Séquences d'attaques pour afficher ses détails sur la page Résultats.

- Total des résultats : indique le nombre total de résultats générés sur votre compte dans la région actuelle. Cela inclut à la fois les résultats individuels et les résultats des séquences d'attaque.

- Ressources contenant des résultats : indique le nombre de ressources associées à une découverte et potentiellement compromises.
- Comptes contenant des résultats : indique le nombre de comptes dans lesquels au moins un résultat a été généré. Si vous êtes un compte autonome, la valeur de ce champ est 1.

Pour les plages de temps Les 7 derniers jours et Les 30 derniers jours, le volet Présentation peut afficher la différence en pourcentage entre les résultats générés semaine après semaine (WoW) ou mois par mois (MoM), respectivement. Si aucun résultat n'a été généré au cours de la semaine ou du mois précédent, en l'absence de données à comparer, il se peut que la différence en pourcentage ne soit pas disponible.



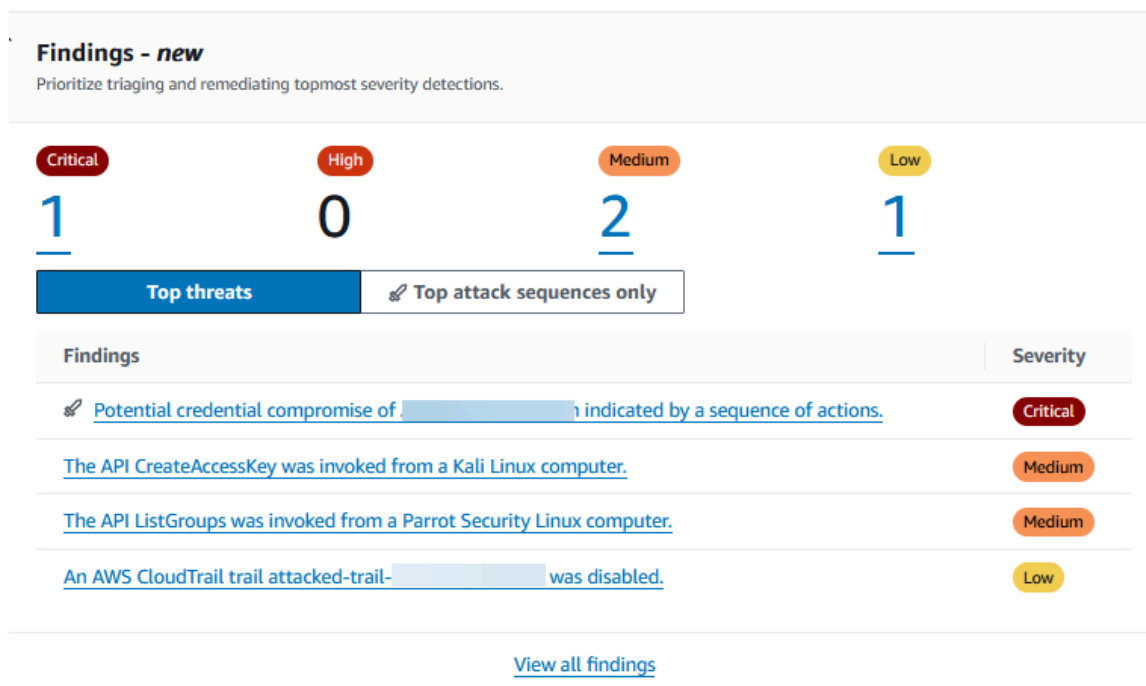
Si vous êtes un compte GuardDuty administrateur, tous ces champs fournissent les données résumées de tous les comptes membres de votre organisation.

Résultats

Le widget Résultats affiche jusqu'à huit résultats principaux. Ces résultats sont répertoriés en fonction de leur niveau de gravité, les résultats critiques étant affichés en premier.

Par défaut, vous pouvez consulter tous les résultats. Pour afficher uniquement les données relatives aux résultats des séquences d'attaque, activez l'option Séquences d'attaque principales uniquement.

Dans cette liste, vous pouvez sélectionner n'importe quelle découverte pour en afficher les détails.



Types de résultat les plus courants

Cette section fournit un graphique circulaire illustrant les cinq types de résultats les plus courants générés dans la région actuelle. Lorsque vous survolez chaque secteur du graphique circulaire, vous pouvez observer les points suivants :

- Nombre de résultats : indique le nombre de fois que ce résultat a été généré dans la plage de dates choisie.
- Gravité : indique le niveau de gravité du résultat.
- Pourcentage : indique la proportion de ce type de résultat par rapport au total.
- Dernière génération : indique le temps écoulé depuis la dernière détection de ce type de recherche.

Résultats par gravité

Cette section affiche un graphique à barres indiquant le nombre total de résultats sur la plage de dates sélectionnée. Le graphique ventile les résultats par gravité (critique, élevé, moyen et faible) et vous aide à visualiser le nombre de résultats à des dates spécifiques comprises dans la fourchette.

Pour afficher les chiffres pour chaque niveau de gravité à une date précise, passez le curseur sur la barre correspondante dans le graphique.

Comptes contenant le plus de résultats

Cette section fournit les données suivantes :

- **Compte** : indique l' Compte AWS identifiant à partir duquel le résultat a été généré.
- **Nombre de résultats** : indique le nombre de fois qu'un résultat a été généré pour cet ID de compte.
- **Dernière génération** : indique le temps écoulé depuis la dernière génération de ce type de résultat pour cet ID de compte.
- **Filtre de gravité** : par défaut, les données sont affichées pour les types de détection de gravité élevée. Les options possibles pour ce champ sont toutes les suivantes : gravité totale, gravité critique, gravité élevée et gravité moyenne.

Ressources contenant des résultats

Cette section fournit les données suivantes :

- **Ressource** : indique le type de ressource potentiellement concerné et si cette ressource appartient à votre compte, vous pouvez accéder au lien rapide pour afficher les détails de la ressource. Si vous êtes GuardDuty administrateur, vous pouvez consulter les détails de la ressource potentiellement affectée en accédant à la GuardDuty console avec les informations d'identification du compte membre propriétaire.
- **Compte** : indique l' Compte AWS ID auquel appartient cette ressource.
- **Nombre de résultats** : indique le nombre de fois que cette ressource a été associée à un résultat.
- **Dernière génération** : indique le temps écoulé depuis la dernière génération d'un type de résultat associé à cette ressource.
- **Filtre de type de ressource** : par défaut, les données sont affichées pour tous les types de ressources. En utilisant ce filtre, vous pouvez choisir d'afficher les données d'un type de ressource spécifique, tel que Instance AccessKey, Lambda, etc.
- **Filtre de gravité** : par défaut, les données sont affichées pour Toutes les sévérités. En utilisant ce filtre, vous pouvez choisir d'afficher les données relatives à d'autres niveaux de gravité. Les options possibles sont les suivantes : gravité critique, gravité élevée, gravité moyenne et gravité totale.

Résultats les moins fréquents

Cette section met en évidence les types qui se produisent rarement dans votre AWS environnement. Ce widget est conçu pour vous aider à identifier et à étudier les modèles de menaces émergents potentiels.

Ce widget affiche les données suivantes :

- Type de recherche : affiche le nom du type de recherche.
- Nombre de résultats : indique le nombre de fois que ce type de résultat a été généré dans la plage de temps choisie.
- Dernière génération : indique le temps écoulé depuis la dernière génération de ce type de résultat.
- Filtre de gravité : par défaut, les données sont affichées pour les types de détection de gravité élevée. Les options possibles pour ce champ sont Sévérité critique, Sévérité élevée, Sévérité moyenne et Sévérité totale.

Couverture des plans de protection

Cette section affiche les statistiques relatives aux comptes des membres de votre organisation. Il indique le nombre de comptes membres qui ont été activés GuardDuty (détection des menaces de base) dans la région actuelle. Seul un GuardDuty administrateur délégué peut consulter les statistiques des comptes des membres au sein de son organisation. Lorsque vous créez une nouvelle AWS organisation, la génération des statistiques pour l'ensemble de l'organisation peut prendre jusqu'à 24 heures.

Comment utiliser ce widget

- Configuration : Si aucun plan de protection n'est configuré, choisissez Configurer dans la colonne Actions.
- Afficher les comptes activés : passez le curseur sur la barre dans la colonne Comptes activés pour voir combien de comptes ont activé chaque plan de protection. Pour consulter davantage les détails du compte, sélectionnez la barre verte, puis choisissez Afficher les comptes.

Protection plans coverage Last updated: 3 hours ago

GuardDuty coverage (foundational)
[4/4 accounts](#)

Protection plan	Enabled accounts	Actions
S3 Protection	<div><div></div></div>	Configure
EKS Protection	<div><div></div></div>	Configure
Runtime monitoring	<div><div></div></div>	<div> <div>Runtime monitoring</div> <div> <div><div></div> Enabled accounts 1</div> <div><div></div> Not enabled accounts 3</div> <div> Configure View accounts </div> </div> </div>
Automated agent management for EKS	<div><div></div></div>	
Automated agent configuration for Fargate (ECS only)	<div><div></div></div>	
Automated agent management for EC2	<div><div></div></div>	Configure
Malware Protection for EC2	<div><div></div></div>	Configure
Lambda Protection	<div><div></div></div>	Configure
RDS Protection	<div><div></div></div>	Configure

Filtrer les résultats dans GuardDuty

Un filtre de recherche vous permet de visualiser les résultats correspondant aux critères que vous spécifiez et de filtrer les résultats non concordants. Vous pouvez facilement créer des filtres de recherche à l'aide de la GuardDuty console Amazon, ou vous pouvez les créer à l'aide de l'[CreateFilter](#) API à l'aide de JSON. Consultez les sections suivantes pour comprendre comment créer un filtre dans la console. Pour utiliser ces filtres afin d'archiver automatiquement les résultats entrants, veuillez consulter [Règles de suppression dans GuardDuty](#).

Lorsque vous créez des filtres, tenez compte de la liste suivante :

- Vous pouvez spécifier un minimum d'un attribut et un maximum de 50 attributs comme critères pour un filtre particulier.
- Lorsque vous utilisez l'opérateur Equals ou Does not equals pour filtrer une valeur d'attribut, telle que l'ID de compte, vous pouvez spécifier un maximum de 50 valeurs.
- Chaque attribut de critères de filtre est évalué en tant qu'opérateur AND. Plusieurs valeurs pour le même attribut sont évaluées comme AND/OR.
- Pour plus d'informations sur le nombre maximal de filtres enregistrés que vous pouvez créer Compte AWS dans chaque filtre Région AWS, voir [GuardDuty quotas](#).

- `service.additionalInfo` Les champs ci-dessous sont spécifiés à l'aide de leur chemin JSON complet, comme tout autre champ. Par exemple : `{ "service.additionalInfo.sample": { "Equals": ["true"] } }`.
- Les champs d'horodatage acceptent des valeurs au format Unix Epoch en millisecondes (par exemple, 1486685375000). Pour une liste complète des champs d'horodatage, consultez la note ci-dessous.

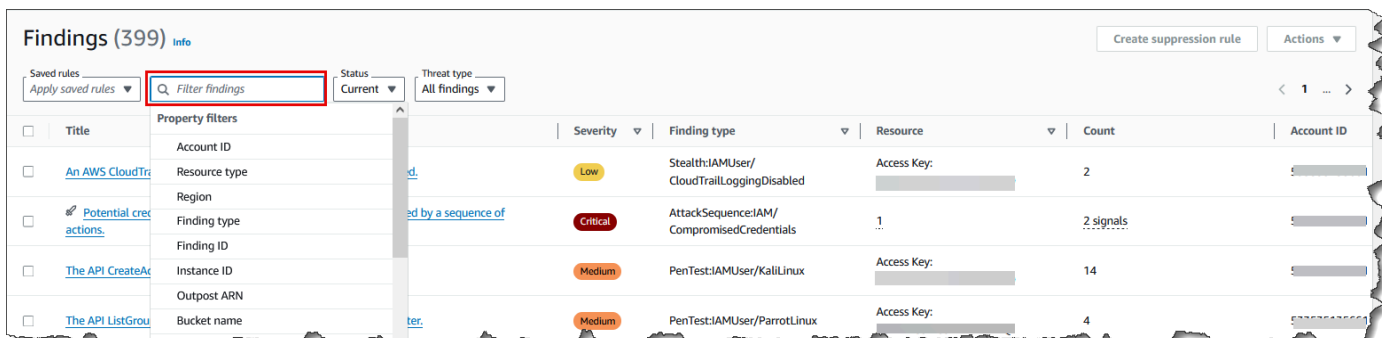
Les sections suivantes fournissent des instructions sur la façon de créer et d'enregistrer des filtres à l'aide de GuardDuty la console, de l'API et de la CLI. Choisissez votre méthode d'accès préférée pour continuer.

Création et enregistrement d'un ensemble de filtres dans la GuardDuty console

Les filtres de recherche peuvent être créés et testés via la GuardDuty console. Vous pouvez enregistrer les filtres créés via la console pour les utiliser dans les règles de suppression ou les futures opérations de filtrage. Un filtre est composé d'au moins un critère de filtre, qui consiste en un attribut de filtre associé à au moins une valeur.

Pour créer et enregistrer des critères de filtre (console)

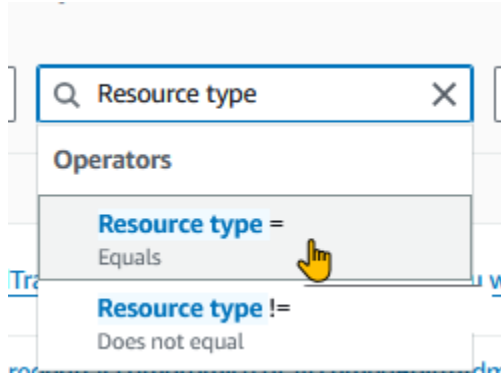
1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le volet de navigation de gauche, sélectionnez Findings.
3. Sur la page Résultats, sélectionnez la barre Filtrer les résultats à côté du menu Règles enregistrées. Cela affichera une liste étendue de filtres de propriétés.



4. Dans la liste étendue des filtres, sélectionnez un attribut en fonction duquel vous souhaitez filtrer le tableau des résultats.

Par exemple, pour afficher les résultats pour lesquels la ressource potentiellement affectée est un S3Bucket, choisissez le type de ressource.

5. Pour les opérateurs, choisissez-en un qui vous aidera à filtrer les résultats pour obtenir le résultat souhaité. Pour continuer l'exemple de l'étape précédente, choisissez Type de ressource =. Cela affichera une liste des types de ressources dans GuardDuty.



Si votre cas d'utilisation nécessite l'exclusion de résultats spécifiques, vous pouvez choisir Does not equal or != opérateur.

6. Spécifiez la valeur du filtre de propriétés sélectionné. Si nécessaire, choisissez Appliquer. Pour continuer l'exemple de l'étape précédente, vous pouvez choisir S3Bucket.

Cela affichera les résultats correspondant aux filtres appliqués.

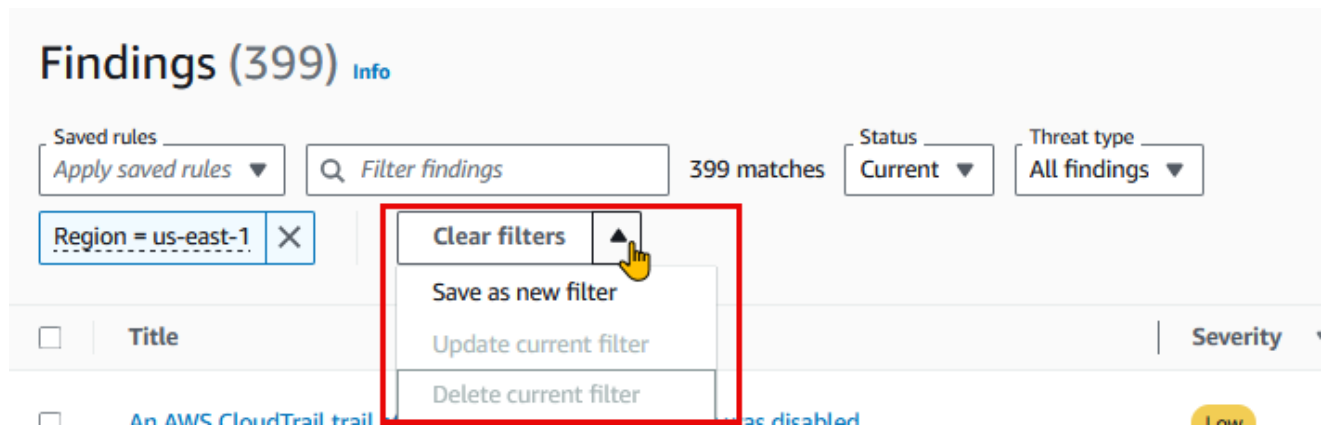
7. Pour ajouter plusieurs critères de filtre, répétez les étapes 3 à 6.

Pour obtenir la liste complète des attributs, voir [Filtres de propriétés dans GuardDuty](#).

8. (Facultatif) enregistrez les attributs et valeurs spécifiés sous forme de filtres

Pour appliquer à nouveau cette combinaison de filtres à l'avenir, vous pouvez enregistrer les attributs spécifiés et leurs valeurs sous forme de jeu de filtres.

- a. Après avoir créé un critère de filtre avec un ou plusieurs filtres de propriétés, sélectionnez la flèche dans le menu Effacer les filtres.



- b. Entrez le nom du jeu de filtres. Le nom doit comporter entre 3 et 64 caractères. Les caractères valides sont les suivants : a-z A-Z, 0-9, point (.), tiret (-) et trait de soulignement (_).
- c. La description est facultative. Si vous entrez une description, elle peut comporter jusqu'à 512 caractères.
- d. Cliquez sur Créer.

Création et enregistrement d'un ensemble de filtres à l'aide de l' GuardDuty API et de la CLI

Vous pouvez créer et tester les filtres de recherche à l'aide des commandes API ou CLI. Un filtre est composé d'au moins un critère de filtre, qui consiste en un attribut de filtre associé à au moins une valeur. Vous pouvez enregistrer des filtres pour créer [Règles de suppression](#) ou effectuer d'autres opérations de filtrage ultérieurement.

Pour créer des filtres de recherche à l'aide de API/CLI

- Exécutez l'[CreateFilter](#) API en utilisant l'ID du détecteur régional de l' Compte AWS endroit où vous souhaitez créer un filtre.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

- Vous pouvez également utiliser la [CLI create-filter](#) pour créer et enregistrer le filtre. Vous pouvez utiliser un ou plusieurs critères de filtre à partir de [Filtres de propriétés dans GuardDuty](#).

Utilisez les exemples suivants en remplaçant les valeurs d'espace réservé indiquées en rouge.

Exemple 1 : créer un nouveau filtre pour afficher tous les résultats correspondant à un type de recherche spécifique

L'exemple suivant crée un filtre qui correspond à tous les PortScan résultats d'une instance créée à partir d'une image spécifique. Les valeurs des espaces réservés sont affichées en rouge. Remplacez ces valeurs par des valeurs adaptées à votre compte. Remplacez-le par l'identifiant `12abc34d567e8fa901bc2d34EXAMPLE` de votre détecteur régional, par exemple.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},  
"resource.instanceDetails.imageId": {"Equals":["ami-0a7a207083example"]}} }'
```

Exemple 2 : créer un nouveau filtre pour afficher tous les résultats correspondant aux niveaux de gravité

L'exemple suivant crée un filtre qui correspond à tous les résultats associés aux niveaux de HIGH gravité. Les valeurs des espaces réservés sont affichées en rouge. Remplacez ces valeurs par des valeurs adaptées à votre compte. Remplacez-le par l'identifiant `12abc34d567e8fa901bc2d34EXAMPLE` de votre détecteur régional, par exemple.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Car API/CLI, [Niveaux de gravité des résultats](#) ils sont représentés par des chiffres. Pour filtrer les résultats en fonction des niveaux de gravité, utilisez les valeurs suivantes :
- Pour les niveaux de LOW gravité, utilisez { "severity": { "Equals": ["1", "2", "3"] } }
- Pour les niveaux de MEDIUM gravité, utilisez { "severity": { "Equals": ["4", "5", "6"] } }
- Pour les niveaux de HIGH gravité, utilisez { "severity": { "Equals": ["7", "8"] } }
- Pour les niveaux de CRITICAL gravité, utilisez { "severity": { "Equals": ["9", "10"] } }

- Pour les résultats présentant plusieurs niveaux de gravité, utilisez des valeurs d'espace réservé similaires à l'exemple suivant : `{ "severity": { "Equals": ["7", "8", "9", "10"] } }`

Cet exemple montre les résultats présentant l'un HIGH ou l'autre des niveaux de CRITICAL gravité.

Note

Si vous spécifiez un exemple avec une seule valeur numérique au lieu de toutes les valeurs numériques associées à un niveau de gravité, l'API et la CLI peuvent afficher les résultats filtrés. Lorsque vous utilisez cet ensemble de filtres enregistré dans la GuardDuty console, il ne fonctionnera pas comme prévu. Cela est dû au fait que la GuardDuty console considère les valeurs du filtre comme CRITICALHIGH,MEDIUM, etLOW. Par exemple, un filtre créé à l'aide d'une commande CLI qui inclut `{ "severity": { "Equals": ["9"] } }` est censé afficher une sortie appropriée dans API/CLI. Toutefois, ce filtre enregistré inclut un niveau de gravité partiel lorsqu'il est utilisé dans la GuardDuty console et n'affichera pas le résultat attendu. Cela oblige l'API et la CLI à spécifier toutes les valeurs associées à chaque niveau de gravité.

Filtrer les métadonnées du cycle de

Lorsque vous récupérez les détails du filtre à l'aide de l'[GetFilter](#) API, vous pouvez consulter les champs de métadonnées du cycle de vie. Ces champs indiquent quand un filtre a été créé et combien de fois il a été modifié.

La `GetFilter` réponse inclut les champs de métadonnées du cycle de vie suivants :

createdAt

Horodatage de la création initiale du filtre. GuardDuty définit cette valeur au moment de la création et ne la modifie jamais. GuardDuty ne renseigne pas ce champ pour les filtres existants (filtres que vous avez créés avant le lancement de cette fonctionnalité).

updatedAt

Horodatage de la dernière mise à jour du filtre. GuardDuty met à jour cette valeur à chaque [UpdateFilter](#) appel réussi. Au moment de la création, des `updatedAt`

`correspondancescreatedAt`. Pour les filtres existants, ce champ n'apparaît qu'après avoir mis à jour le filtre au moins une fois.

version

Nombre entier qui compte le nombre de fois que vous avez modifié le filtre. Il commence à 1 lorsque vous créez le filtre et augmente de 1 à chaque `UpdateFilter` appel réussi, que le contenu du filtre change ou non. GuardDuty ne renseigne pas ce champ pour les anciens filtres.

Note

Ces champs de métadonnées du cycle de vie sont en lecture seule. Les `UpdateFilter` opérations `CreateFilter` et n'acceptent pas ces champs en entrée, et leurs réponses ne les incluent pas. Pour consulter les métadonnées du cycle de vie, appelez `GetFilter`.

Filtres de propriétés dans GuardDuty

Lorsque vous créez des filtres ou que vous trie des résultats à l'aide des opérations d'API, vous devez spécifier des critères de filtre au format JSON. Ces critères de filtre sont en corrélation avec le JSON détaillé d'un résultat. Le tableau suivant contient la liste des noms d'affichage de la console pour les attributs de filtre et leurs noms de champs JSON équivalents.

Nom de champ de console	Nom de champ JSON
ID de compte	<code>accountId</code>
ID de résultat	<code>id</code>
Région	<code>region</code>
Sévérité	<code>severity</code> Vous pouvez filtrer les types de résultats en fonction de leur niveau de gravité. Pour plus d'informations sur les valeurs de gravité, consultez Niveaux de gravité des GuardDuty résultats . Si vous l'utilisez <code>severity</code> avec API AWS CLI, ou CloudFormation, une valeur

Nom de champ de console	Nom de champ JSON
	numérique lui est attribuée. Pour plus d'informations, consultez FindingCriteria dans le Amazon GuardDuty API Reference.
Type de résultat	type
Nom de règle de détection personnalisé	personnalisé DetectionRuleName Présent uniquement sur les résultats générés par une règle de détection personnalisée de surveillance du temps d'exécution. Pour plus d'informations, consultez Résultats des règles de surveillance du temps d'exécution .
Mis à jour le	updatedAt
ID de clé d'accès	ressource.access KeyDetails.accessKeyId
ID principal	ressource.access KeyDetails.principalId
Nom d'utilisateur	ressource.access KeyDetails.userName
Type utilisateur	ressource.access KeyDetails.userType
ID de profil d'instance IAM	ressource.instance Details.iamInstanceProfile.id
ID d'instance	ressource.instance Details.instanceId
ID d'image d'instance	ressource.instance Details.imageId
Clé de balise d'instance	ressource.instance Details.tags.key
Valeur de balise d'instance	ressource.instance Details.tags.value
Adresse IPv6	ressource.instance Details.networkInterfaces.ipv6Addresses

Nom de champ de console	Nom de champ JSON
Adresse IPv4 privée	ressource.instance Details.networkInterfaces.p rivatelpAddresses.privatelpAddress
Nom DNS public	ressource.instance Details.networkInterfaces.p ublicDnsName
Adresse IP publique	ressource.instance Details.networkInterfaces.p ublicIp
ID du groupe de sécurité	ressource.instance Details.networkInterfaces.s ecurityGroups.groupId
Nom du groupe de sécurité	ressource.instance Details.networkInterfaces.s ecurityGroups.groupName
ID de sous-réseau (subnet)	ressource.instance Details.networkInterfaces.s ubnetId
ID du VPC	ressource.instance Details.networkInterfaces.v pcId
ARN d'Outpost	ressource.instance Details.outpostARN
Type de ressource	resource.resourceType
Autorisations du compartiment	ressource.s3 BucketDetails.publicAccess. effectivePermission
Nom du compartiment	ressource.s3 BucketDetails.name
Clé de balise du compartiment	ressource.s3 BucketDetails.tags.key
Valeur de balise de compartiment	ressource.s3 BucketDetails.tags.value
Type de compartiment	ressource.s3 BucketDetails.type
Type d'action	service.action.actionType
API appelée	service.action.aws ApiCallAction.api

Nom de champ de console	Nom de champ JSON
Type d'appelant d'API	service.action.aws ApiCallAction.callerType
Code d'erreur d'API	service.action.aws ApiCallAction.errorCode
Ville de l'appelant d'API	service.action.aws ApiCallAction.remoteIpDetails.city.cityName
Pays de l'appelant d'API	service.action.aws ApiCallAction.remoteIpDetails.country.countryName
Adresse IPv4 de l'appelant d'API	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV4
Adresse IPv6 de l'appelant de l'API	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV6
ID ASN de l'appelant d'API	service.action.aws ApiCallAction.remoteIpDetails.organization.asn
Nom ASN de l'appelant d'API	service.action.aws ApiCallAction.remoteIpDetails.organization.asnOrg
Nom du service de l'appelant d'API	service.action.aws ApiCallAction.serviceName
Domaine de demande DNS	service.action.dns RequestAction.domain
Suffixe de domaine de demande DNS	service.action.dns RequestAction.domainWithSuffix
Connexion réseau bloquée	service.action.network ConnectionAction.blocked
Direction de la connexion réseau	service.action.network ConnectionAction.connectionDirection
Port local de la connexion réseau	service.action.network ConnectionAction.localPortDetails.port

Nom de champ de console	Nom de champ JSON
Protocole de la connexion réseau	service.action.network ConnectionAction.p rotocol
Ville de la connexion réseau	service.action.network ConnectionAction.r emoteIpDetails.city.cityName
Pays de la connexion réseau	service.action.network ConnectionAction.r emoteIpDetails.country.countryName
Adresse IPv4 distante de la connexion réseau	service.action.network ConnectionAction.r emoteIpDetails.ipAddressV4
Adresse IPv6 distante de connexion réseau	service.action.network ConnectionAction.r emoteIpDetails.ipAddressV6
ID ASN de l'adresse IP distante de la connexion réseau	service.action.network ConnectionAction.r emoteIpDetails.organization.asn
Nom ASN de l'adresse IP distante de la connexion réseau	service.action.network ConnectionAction.r emoteIpDetails.organization.asnOrg
Port distant de la connexion réseau	service.action.network ConnectionAction.r emotePortDetails.port
Compte distant affilié	service.action.aws ApiCallAction.remo teAccountDetails.affiliated
Adresse IPv4 de l'appelant de l'API Kubernetes	service.action.kubernetes ApiCallAction.remo teIpDetails.ipAddressV4
Adresse IPv6 de l'appelant de l'API Kubernetes	service.action.kubernetes ApiCallAction.remo teIpDetails.ipAddressV6
Espace de noms Kubernetes	service.action.kubernetes ApiCallAction.name space
ID ASN de l'appelant de l'API Kubernetes	service.action.kubernetes ApiCallAction.remo teIpDetails.organization.asn

Nom de champ de console	Nom de champ JSON
URI de demande d'appel d'API Kubernetes	service.action.kubernetes ApiCallAction.requestUri
Code d'état de l'API Kubernetes	service.action.kubernetes ApiCallAction.statusCode
Adresse IPv4 locale de connexion réseau	service.action.network ConnectionAction.localIpDetails.ipAddressV4
Adresse IPv6 locale de connexion réseau	service.action.network ConnectionAction.localIpDetails.ipAddressV6
Protocole	service.action.network ConnectionAction.protocol
Nom du service de l'appel d'API	service.action.aws ApiCallAction.serviceName
ID du compte de l'appelant d'API	service.action.aws ApiCallAction.remoteAccountDetails.accountId
Nom de la liste des menaces	service.additional Info.threatListName
Rôle de ressource	service.resourceRole
Nom du cluster EKS	ressource.eks ClusterDetails.name
Nom de charge de travail Kubernetes	ressource.kubernetes Details.kubernetes WorkloadDetails.name
Espace de noms de charge de travail Kubernetes	ressource.kubernetes Details.kubernetes WorkloadDetails.namespace
Nom d'utilisateur Kubernetes	ressource.kubernetes Details.kubernetes UserDetails.username
Image de conteneur Kubernetes	ressource.kubernetes Details.kubernetes WorkloadDetails.containers.image

Nom de champ de console	Nom de champ JSON
Préfixe de l'image de conteneur Kubernetes	ressource.kubernetes Details.kubernetes WorkloadDetails.containers.imagePrefix
ID de numérisation	service.ebs VolumeScanDetails.scanId
Nom de la menace EBS Volume Scan	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name
Nom de la menace de scan d'objets S3	service .malware ScanDetails.threats.name
Gravité de la menace	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity
Fichier SHA	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
Nom du cluster ECS	ressource.ecs ClusterDetails.name
Image de conteneur ECS	ressource.ecs ClusterDetails.taskDetails.containers.image
ARN de définition de tâche ECS	ressource.ecs ClusterDetails.taskDetails.definitionArn
Image de conteneur autonome	ressource.container Details.image
ID d'instance de base de données	ressource.rds DbInstanceDetails.dbInstanceIdentifier
ID de cluster de base de données	ressource.rds DbInstanceDetails.dbClusterIdentifier
Moteur de base de données	ressource.rds DbInstanceDetails.engine
Utilisateur de la base de donnée	ressource.rds DbUserDetails.user

Nom de champ de console	Nom de champ JSON
Exécutable SHA-256	service.runtime Details.process.executableSHA256
Nom du processus	service.runtime Details.process.name
Chemin exécutable	service.runtime Details.process.executablePath
Nom de fonction Lambda	ressource.lambda Details.functionName
ARN de fonction Lambda	ressource.lambda Details.functionArn
Clé de balise de fonction Lambda	ressource.lambda Details.tags.key
Valeur de balise de fonction Lambda	ressource.lambda Details.tags.value
Domaine de demande DNS	service.action.dns RequestAction.domainWithSuffix

Tous les autres champs de recherche (répertoriés ci-dessous) sont uniquement disponibles en tant que critères de filtrage des règles de suppression (en utilisant [CreateFilter](#) et [UpdateFilter](#)). Ces champs ne sont pas pris en charge par d'autres opérations d'API. Les règles de suppression qui utilisent ces champs doivent être créées ou mises à jour via l'API. Ces champs ne peuvent être appliqués qu'aux filtres comportant une ARCHIVE action.

Note

Les champs suivants acceptent les valeurs d'horodatage au format Unix Epoch en millisecondes (par exemple, cela 1262309025000 représente le vendredi 1er janvier 2010 à 1 h 23 h 45 GMT) :

- createdAt
- updatedAt
- service.événement FirstSeen
- service.événement LastSeen
- ressource.instance Details.launchTime
- ressource.lambda Details.lastModifiedAt
- ressource.s3 BucketDetails.createdAt

- ressource.eks ClusterDetails.createdAt
- ressource.ecs ClusterDetails.taskDetails.createdAt
- ressource.ecs ClusterDetails.taskDetails.startedAt
- service.ebs VolumeScanDetails.scanStartedAt
- service.ebs VolumeScanDetails.scanCompletedAt
- service.runtime Details.context.modifiedAt
- service.runtime Details.context.modifyingProcess.startTime
- service.runtime Details.context.modifyingProcess.lineage.startTime
- service.runtime Details.context.targetProcess.startTime
- service.runtime Details.context.targetProcess.lineage.startTime
- service.runtime Details.process.startTime
- service.runtime Details.process.lineage.startTime
- Service.Detection.Sequence.actors.Session.CreatedTime
- Service.Detection.Sequence.signals.CreatedAt
- service.detection.sequence.signals.Updatedat
- service.detection.sequence.signals.first SeenAt
- service.detection.sequence.signals.last SeenAt
- service.detection.sequence.resources.data.s3 Bucket.createdAt
- service.detection.sequence.resources.data.ecs Task.createdAt
- service.detection.sequence.resources.data.eks Cluster.createdAt

Nom de champ JSON

arn

associé AttackSequenceArn

createdAt

partition

ressource.access KeyDetails.userIdentity.accessKeyId

ressource.access KeyDetails.userIdentity.accountId

ressource.access KeyDetails.userIdentity.arn

Nom de champ JSON

ressource.access KeyDetails.userIdentity.principalId

ressource.access KeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated

ressource.access KeyDetails.userIdentity.sessionContext.ec2RoleDelivery

ressource.access KeyDetails.userIdentity.sessionContext.invokedBy

ressource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.accountId

ressource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.arn

ressource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.principalId

ressource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.type

ressource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.userName

ressource.access KeyDetails.userIdentity.sessionContext.sourceIdentity

ressource.access KeyDetails.userIdentity.sessionContext.webIdFederationData.attributes

ressource.access KeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider

ressource.access KeyDetails.userIdentity.type

ressource.access KeyDetails.userIdentity.userName

ressource.bedrock GuardrailDetails.guardrailArn

ressource.bedrock GuardrailDetails.guardrailVersion

ressource.container Details.containerRuntime

ressource.container Details.imagePrefix

ressource.container Details.securityContext.allowPrivilegeEscalation

ressource.container Details.securityContext.privileged

Nom de champ JSON

ressource.container Details.volumeMounts.mountPath

ressource.container Details.volumeMounts.name

ressource.ebs VolumeDetails.scannedVolumeDetails.deviceName

ressource.ebs VolumeDetails.scannedVolumeDetails.encryptionType

ressource.ebs VolumeDetails.scannedVolumeDetails.kmsKeyArn

ressource.ebs VolumeDetails.scannedVolumeDetails.snapshotArn

ressource.ebs VolumeDetails.scannedVolumeDetails.volumeArn

ressource.ebs VolumeDetails.scannedVolumeDetails.volumeSizeInGB

ressource.ebs VolumeDetails.scannedVolumeDetails.volumeType

ressource.ebs VolumeDetails.skippedVolumeDetails.deviceName

ressource.ebs VolumeDetails.skippedVolumeDetails.encryptionType

ressource.ebs VolumeDetails.skippedVolumeDetails.kmsKeyArn

ressource.ebs VolumeDetails.skippedVolumeDetails.snapshotArn

ressource.ebs VolumeDetails.skippedVolumeDetails.volumeArn

ressource.ebs VolumeDetails.skippedVolumeDetails.volumeSizeInGB

ressource.ebs VolumeDetails.skippedVolumeDetails.volumeType

ressource.ecs ClusterDetails.activeServicesCount

ressource.ecs ClusterDetails.arn

ressource.ecs ClusterDetails.registeredContainerInstancesCount

ressource.ecs ClusterDetails.runningTasksCount

Nom de champ JSON

ressource.ecs ClusterDetails.status

ressource.ecs ClusterDetails.tags.key

ressource.ecs ClusterDetails.tags.value

ressource.ecs ClusterDetails.taskDetails.arn

ressource.ecs ClusterDetails.taskDetails.containers.containerRuntime

ressource.ecs ClusterDetails.taskDetails.containers.id

ressource.ecs ClusterDetails.taskDetails.containers.imagePrefix

ressource.ecs ClusterDetails.taskDetails.containers.name

ressource.ecs ClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation

ressource.ecs ClusterDetails.taskDetails.containers.securityContext.privileged

ressource.ecs ClusterDetails.taskDetails.containers.volumeMounts.mountPath

ressource.ecs ClusterDetails.taskDetails.containers.volumeMounts.name

ressource.ecs ClusterDetails.taskDetails.createdAt

ressource.ecs ClusterDetails.taskDetails.group

ressource.ecs ClusterDetails.taskDetails.launchType

ressource.ecs ClusterDetails.taskDetails.startedAt

ressource.ecs ClusterDetails.taskDetails.startedBy

ressource.ecs ClusterDetails.taskDetails.tags.key

ressource.ecs ClusterDetails.taskDetails.tags.value

ressource.ecs ClusterDetails.taskDetails.version

Nom de champ JSON

ressource.ecs ClusterDetails.taskDetails.volumes.hostPath.path

ressource.ecs ClusterDetails.taskDetails.volumes.name

ressource.eks ClusterDetails.arn

ressource.eks ClusterDetails.createdAt

ressource.eks ClusterDetails.status

ressource.eks ClusterDetails.tags.key

ressource.eks ClusterDetails.tags.value

ressource.eks ClusterDetails.vpcId

ressource.instance Details.iamInstanceProfile.arn

ressource.instance Details.instanceState

ressource.instance Details.instanceType

ressource.instance Details.launchTime

ressource.instance Details.networkInterfaces.networkInterfaceId

ressource.instance Details.networkInterfaces.privateDnsName

ressource.instance Details.networkInterfaces.privateIpAddress

ressource.instance Details.networkInterfaces.privateIpAddresses.privateDnsName

ressource.instance Details.platform

ressource.instance Details.productCodes.productCodeId

ressource.instance Details.productCodes.productCodeType

ressource.kubernetes Details.kubernetesUserDetails.groups

Nom de champ JSON

ressource.kubernetes Details.kubernetesUserDetails.impersonatedUser.groups

ressource.kubernetes Details.kubernetesUserDetails.impersonatedUser.username

ressource.kubernetes Details.kubernetesUserDetails.sessionName

ressource.kubernetes Details.kubernetesUserDetails.uid

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.containerRuntime

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.id

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.name

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEscalation

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.privileged

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.mountPath

ressource.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.name

ressource.kubernetes Details.kubernetesWorkloadDetails.hostIpc

ressource.kubernetes Details.kubernetesWorkloadDetails.hostNetwork

ressource.kubernetes Details.kubernetesWorkloadDetails.hostPid

ressource.kubernetes Details.kubernetesWorkloadDetails.serviceAccountName

ressource.kubernetes Details.kubernetesWorkloadDetails.type

ressource.kubernetes Details.kubernetesWorkloadDetails.uid

ressource.kubernetes Details.kubernetesWorkloadDetails.volumes.hostPath.path

ressource.kubernetes Details.kubernetesWorkloadDetails.volumes.name

ressource.lambda Details.description

Nom de champ JSON

ressource.lambda Details.lastModifiedAt

ressource.lambda Details.revisionId

ressource.lambda Details.vpcConfig.securityGroups.groupId

ressource.lambda Details.vpcConfig.securityGroups.groupName

ressource.lambda Details.vpcConfig.subnetIds

ressource.lambda Details.vpcConfig.vpcId

ressource.rds DbInstanceDetails.dbInstanceArn

ressource.rds DbInstanceDetails.dbiResourceId

ressource.rds DbInstanceDetails.dbSecurityGroups.name

ressource.rds DbInstanceDetails.dbSecurityGroups.status

ressource.rds DbInstanceDetails.engineVersion

ressource.rds DbInstanceDetails.iamDatabaseAuthenticationEnabled

ressource.rds DbInstanceDetails.publiclyAccessible

ressource.rds DbInstanceDetails.vpcId

ressource.rds DbInstanceDetails.vpcSecurityGroups.status

ressource.rds DbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId

ressource.rds DbUserDetails.application

ressource.rds DbUserDetails.authMethod

ressource.rds DbUserDetails.database

ressource.rds DbUserDetails.ssl

Nom de champ JSON

ressource.rds LimitlessDbDetails.dbClusterIdentifier

ressource.rds LimitlessDbDetails.dbShardGroupArn

ressource.rds LimitlessDbDetails.dbShardGroupIdentifier

ressource.rds LimitlessDbDetails.dbShardGroupResourceId

ressource.rds LimitlessDbDetails.engine

ressource.rds LimitlessDbDetails.engineVersion

ressource.rds LimitlessDbDetails.tags.key

ressource.rds LimitlessDbDetails.tags.value

ressource.s3 BucketDetails.arn

ressource.s3 BucketDetails.createdAt

ressource.s3 BucketDetails.defaultServerSideEncryption.encryptionType

ressource.s3 BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn

ressource.s3 BucketDetails.owner.id

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicAcls

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicPolicy

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.ignorePublicAcls

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.restrictPublicBuckets

Nom de champ JSON

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicReadAccess

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicWriteAccess

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicAcls

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicPolicy

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.ignorePublicAcls

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess

ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess

ressource.s3 BucketDetails.s3ObjectDetails.eTag

ressource.s3 BucketDetails.s3ObjectDetails.hash

ressource.s3 BucketDetails.s3ObjectDetails.key

ressource.s3 BucketDetails.s3ObjectDetails.objectArn

ressource.s3 BucketDetails.s3ObjectDetails.versionId

schemaVersion

service.action.aws ApiCallAction.domainDetails.domain

service.action.aws ApiCallAction.remoteIpDetails.country.countryCode

Nom de champ JSON

service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lat

service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lon

service.action.aws ApiCallAction.remoteIpDetails.organization.isp

service.action.aws ApiCallAction.remoteIpDetails.organization.org

service.action.aws ApiCallAction.userAgent

service.action.dns RequestAction.blocked

service.action.dns RequestAction.protocol

service.action.kubernetes ApiCallAction.parameters

service.action.kubernetes ApiCallAction.remoteIpDetails.country.countryCode

service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lat

service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lon

service.action.kubernetes ApiCallAction.resource

service.action.kubernetes ApiCallAction.resourceName

service.action.kubernetes ApiCallAction.sourceIPs

service.action.kubernetes ApiCallAction.subresource

service.action.kubernetes ApiCallAction.userAgent

service.action.kubernetes ApiCallAction.verb

service.action.kubernetes PermissionCheckedDetails.allowed

service.action.kubernetes PermissionCheckedDetails.namespace

service.action.kubernetes PermissionCheckedDetails.resource

Nom de champ JSON

service.action.kubernetes PermissionCheckedDetails.verb

service.action.kubernetes RoleBindingDetails.kind

service.action.kubernetes RoleBindingDetails.name

service.action.kubernetes RoleBindingDetails.roleRefKind

service.action.kubernetes RoleBindingDetails.roleRefName

service.action.kubernetes RoleBindingDetails.uid

service.action.kubernetes RoleDetails.kind

service.action.kubernetes RoleDetails.name

service.action.kubernetes RoleDetails.uid

service.action.network ConnectionAction.localNetworkInterface

service.action.network ConnectionAction.localPortDetails.portName

service.action.network ConnectionAction.remoteIpDetails.country.countryCode

service.action.network ConnectionAction.remoteIpDetails.geoLocation.lat

service.action.network ConnectionAction.remoteIpDetails.geoLocation.lon

service.action.network ConnectionAction.remoteIpDetails.organization.isp

service.action.network ConnectionAction.remoteIpDetails.organization.org

service.action.network ConnectionAction.remotePortDetails.portName

service.action.port ProbeAction.blocked

service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV4

service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV6

Nom de champ JSON

service.action.port ProbeAction.portProbeDetails.localPortDetails.port

service.action.port ProbeAction.portProbeDetails.localPortDetails.portName

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.city.cityName

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryCode

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryName

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asn

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.isp

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.org

service.action.rds LoginAttemptAction.loginAttributes.application

service.action.rds LoginAttemptAction.loginAttributes.failedLoginAttempts

service.action.rds LoginAttemptAction.loginAttributes.successfulLoginAttempts

service.action.rds LoginAttemptAction.loginAttributes.user

service.action.rds LoginAttemptAction.remoteIpDetails.city.cityName

service.action.rds LoginAttemptAction.remoteIpDetails.country.countryCode

service.action.rds LoginAttemptAction.remoteIpDetails.country.countryName

Nom de champ JSON

service.action.rds LoginAttemptAction.remotelpDetails.geoLocation.lat

service.action.rds LoginAttemptAction.remotelpDetails.geoLocation.lon

service.action.rds LoginAttemptAction.remotelpDetails.ipAddressV4

service.action.rds LoginAttemptAction.remotelpDetails.ipAddressV6

service.action.rds LoginAttemptAction.remotelpDetails.organization.asn

service.action.rds LoginAttemptAction.remotelpDetails.organization.asnOrg

service.action.rds LoginAttemptAction.remotelpDetails.organization.isp

service.action.rds LoginAttemptAction.remotelpDetails.organization.org

service.additional Info.agentDetails.agentId

service.additional Info.agentDetails.agentVersion

service.additional Info.anomalies.anomalousAPIs

service.additional Info.authenticationMethod

service.additional Info.averagePacketSizeIn

service.additional Info.averagePacketSizeOut

service.additional Info.context

service.additional Info.domain

service.additional Info.inBytes

service.additional Info.localNetworkInterfaceOwner

service.additional Info.localPort

service.additional Info.outBytes

Nom de champ JSON

service.additional Info.packetsIn

service.additional Info.packetsOut

service.additional Info.policyArn

service.additional Info.policyName

service.additional Info.remotePort

service.additional Info.sample

service.additional Info.scannedPort

service.additional Info.threatFileSha256

service.additional Info.threatName

service.additional Info.totalBytesIn

service.additional Info.totalBytesOut

service.additional Info.type

service.additional Info.unusual.asnOrg

service.additional Info.unusual.port

service.additional Info.unusualProtocol

service.additional Info.userAgent.fullUserAgent

service.additional Info.userAgent.userAgentCategory

service.additional Info.value

service.additional Info.vpcOwnerAccountId

service.count

Nom de champ JSON

service.detection.sequence.actors.id

service.detection.sequence.actors.process.name

service.detection.sequence.actors.process.path

service.detection.sequence.actors.process.sha256

Service.Detection.Sequence.Actors.Session.CreatedTime

service.detection.sequence.actors.session.issuer

statut Service.Detection.Sequence.Actors.Session.MFAstatus

service.detection.sequence.actors.session.uid

service.detection.sequence.actors.user.account.account

service.detection.sequence.actors.user.account.uid

service.detection.sequence.actors.user.CredentialUid

service.detection.sequence.actors.user.name

service.detection.sequence.actors.user.type

service.detection.sequence.actors.user.uid

service.detection.sequence.additional SequenceTypes

service.detection.sequence.description

service.detection.sequence.endpoints.autonomous System.name

service.detection.sequence.endpoints.autonomous System.number

service.detection.sequence.endpoints.connection.direction

service.detection.sequence.endpoints.domain

Nom de champ JSON

service.detection.sequence.endpoints.id

service.detection.sequence.endpoints.ip

service.detection.sequence.endpoints.location.city

service.detection.sequence.endpoints.location.country

service.detection.sequence.endpoints.location.lat

service.detection.sequence.endpoints.location.lon

service.detection.sequence.endpoints.port

Service.Detection.Sequence.Resources.AccountId

Service.Detection.Sequence.Resources.CloudPartition

service.detection.sequence.resources.data.access Key.principalId

service.detection.sequence.resources.data.access Key.userName

service.detection.sequence.resources.data.access Key.userType

service.detection.sequence.resources.data.autoscaling AutoScalingGroup.ec2InstanceUids

service.detection.sequence.resources.data.cloudformation Stack.ec2InstanceUids

service.detection.sequence.resources.data.container.image

Service.Detection.Sequence.Resources.Data.Container.ImageUid

service.detection.sequence.resources.data.ec2 Image.ec2InstanceUids

service.detection.sequence.resources.data.ec2 Instance.availabilityZone

service.detection.sequence.resources.data.ec2 Instance.ec2NetworkInterfaceUids

service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.arn

Nom de champ JSON

service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.id

service.detection.sequence.resources.data.ec2 Instance.imageDescription

service.detection.sequence.resources.data.ec2 Instance.instanceState

service.detection.sequence.resources.data.ec2 Instance.instanceType

service.detection.sequence.resources.data.ec2 Instance.outpostArn

service.detection.sequence.resources.data.ec2 Instance.platform

service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeId

service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeType

service.detection.sequence.resources.data.ec2 LaunchTemplate.ec2InstanceUids

service.detection.sequence.resources.data.ec2 LaunchTemplate.version

service.detection.sequence.resources.data.ec2 NetworkInterface.ipv6Addresses

service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateDnsName

service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateIpAddress

service.detection.sequence.resources.data.ec2 NetworkInterface.publicIp

service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupId

service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupName

service.detection.sequence.resources.data.ec2 NetworkInterface.subnetId

service.detection.sequence.resources.data.ec2 NetworkInterface.vpcId

service.detection.sequence.resources.data.ec2 Vpc.ec2InstanceUids

Nom de champ JSON

service.detection.sequence.resources.data.ecs Cluster.ec2InstanceUids

service.detection.sequence.resources.data.ecs Cluster.status

service.detection.sequence.resources.data.ecs Task.containerUids

service.detection.sequence.resources.data.ecs Task.createdAt

service.detection.sequence.resources.data.ecs Task.launchType

service.detection.sequence.resources.data.ecs Task.taskDefinitionArn

service.detection.sequence.resources.data.eks Cluster.arn

service.detection.sequence.resources.data.eks Cluster.createdAt

service.detection.sequence.resources.data.eks Cluster.ec2InstanceUids

service.detection.sequence.resources.data.eks Cluster.status

service.detection.sequence.resources.data.eks Cluster.vpcId

service.detection.sequence.resources.data.iam InstanceProfile.ec2InstanceUids

service.detection.sequence.resources.data.iam InstanceProfile.id

service.detection.sequence.resources.data.kubernetes Workload.containerUids

service.detection.sequence.resources.data.kubernetes Workload.namespace

service.detection.sequence.resources.data.kubernetes Workload.type

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclAccess

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclIgnoreBehavior

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicBucketRestrictBehavior

Nom de champ JSON

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicPolicyAccess

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclAccess

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclIgnoreBehavior

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicBucketRestrictBehavior

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicPolicyAccess

service.detection.sequence.resources.data.s3 Bucket.createdAt

service.detection.sequence.resources.data.s3 Bucket.effectivePermission

service.detection.sequence.resources.data.s3 Bucket.encryptionKeyArn

service.detection.sequence.resources.data.s3 Bucket.encryptionType

service.detection.sequence.resources.data.s3 Bucket.ownerId

service.detection.sequence.resources.data.s3 Bucket.publicReadAccess

service.detection.sequence.resources.data.s3 Bucket.publicWriteAccess

service.detection.sequence.resources.data.s3 Bucket.s3ObjectUids

service.detection.sequence.resources.data.s3 Object.eTag

service.detection.sequence.resources.data.s3 Object.key

service.detection.sequence.resources.data.s3 Object.versionId

service.detection.sequence.resources.name

service.detection.sequence.resources.region

Service.Detection.Sequence.Resources.ResourceType

Nom de champ JSON

service.detection.sequence.resources.service

service.detection.sequence.resources.tags.key

service.detection.sequence.resources.tags.value

service.detection.sequence.resources.uid

service.detection.sequence.sequence Indicators.key

service.detection.sequence.sequence Indicators.title

service.detection.sequence.sequence Indicators.values

Service.Detection.Sequence.Signals.ActorIds

service.detection.sequence.signals.count

Service.Detection.Sequence.Signals.CreatedAt

service.detection.sequence.signals.description

Service.Detection.Sequence.Signals.EndpointIds

service.detection.sequence.signals.first SeenAt

service.detection.sequence.signals.last SeenAt

service.detection.sequence.signals.name

Service.Detection.Sequence.Signals.ResourceUids

service.detection.sequence.signals.severity

service.detection.sequence.signals.signal Indicators.key

service.detection.sequence.signals.signal Indicators.title

service.detection.sequence.signals.signal Indicators.values

Nom de champ JSON

service.detection.sequence.signals.type

service.detection.sequence.signals.uid

service.detection.sequence.signals.Updatedat

service.detection.sequence.uid

Service.detectorID

service.ebs VolumeScanDetails.scanCompletedAt

service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.count

service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity

service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName

service.ebs VolumeScanDetails.scanDetections.scannedItemCount.files

service.ebs VolumeScanDetails.scanDetections.scannedItemCount.totalGb

service.ebs VolumeScanDetails.scanDetections.scannedItemCount.volumes

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.itemCount

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.shortened

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePath.fileName

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePath.filePath

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePath.volumeArn

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount

service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount

Nom de champ JSON

service.ebs VolumeScanDetails.scanDetections.threatsDetectedItemCount.files

service.ebs VolumeScanDetails.scanStartedAt

service.ebs VolumeScanDetails.scanType

service.ebs VolumeScanDetails.sources

service.événement FirstSeen

service.événement LastSeen

service .malware ScanDetails.scanCategory

service .malware ScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn

service .malware ScanDetails.scanConfiguration.triggerType

service .malware ScanDetails.threats.count

service .malware ScanDetails.threats.hash

service .malware ScanDetails.threats.itemDetails.additionalInfo.deviceName

service .malware ScanDetails.threats.itemDetails.additionalInfo.versionId

service .malware ScanDetails.threats.itemDetails.hash

service .malware ScanDetails.threats.itemDetails.itemPath

service .malware ScanDetails.threats.itemDetails.resourceArn

service .malware ScanDetails.threats.itemPaths.hash

service .malware ScanDetails.threats.itemPaths.nestedItemPath

service .malware ScanDetails.threats.source

service .malware ScanDetails.uniqueThreatCount

Nom de champ JSON

service.runtime Details.context.addressFamily

service.runtime Details.context.commandLineExample

service.runtime Details.context.fileSystemType

service.runtime Details.context.flags

service.runtime Details.context.ianaProtocolNumber

service.runtime Details.context.ldPreloadValue

service.runtime Details.context.libraryPath

service.runtime Details.context.memoryRegions

service.runtime Details.context.modifiedAt

service.runtime Details.context.modifyingProcess.euid

service.runtime Details.context.modifyingProcess.executablePath

service.runtime Details.context.modifyingProcess.executableSha256

service.runtime Details.context.modifyingProcess.lineage.euid

service.runtime Details.context.modifyingProcess.lineage.executablePath

service.runtime Details.context.modifyingProcess.lineage.name

service.runtime Details.context.modifyingProcess.lineage.namespacePid

service.runtime Details.context.modifyingProcess.lineage.parentUuid

service.runtime Details.context.modifyingProcess.lineage.pid

service.runtime Details.context.modifyingProcess.lineage.startTime

service.runtime Details.context.modifyingProcess.lineage.userId

Nom de champ JSON

service.runtime Details.context.modifyingProcess.lineage.uuid

service.runtime Details.context.modifyingProcess.name

service.runtime Details.context.modifyingProcess.namespacePid

service.runtime Details.context.modifyingProcess.parentUuid

service.runtime Details.context.modifyingProcess.pid

service.runtime Details.context.modifyingProcess.pwd

service.runtime Details.context.modifyingProcess.startTime

service.runtime Details.context.modifyingProcess.user

service.runtime Details.context.modifyingProcess.userId

service.runtime Details.context.modifyingProcess.uuid

service.runtime Details.context.mountSource

service.runtime Details.context.mountTarget

service.runtime Details.context.relatedFilePaths

service.runtime Details.context.releaseAgentPath

service.runtime Details.context.runcBinaryPath

service.runtime Details.context.scriptPath

service.runtime Details.context.serviceName

service.runtime Details.context.shellHistoryFilePath

service.runtime Details.context.socketPath

service.runtime Details.context.targetProcess.euid

Nom de champ JSON

service.runtime Details.context.targetProcess.executablePath

service.runtime Details.context.targetProcess.executableSha256

service.runtime Details.context.targetProcess.lineage.euid

service.runtime Details.context.targetProcess.lineage.executablePath

service.runtime Details.context.targetProcess.lineage.name

service.runtime Details.context.targetProcess.lineage.namespacePid

service.runtime Details.context.targetProcess.lineage.parentUuid

service.runtime Details.context.targetProcess.lineage.pid

service.runtime Details.context.targetProcess.lineage.startTime

service.runtime Details.context.targetProcess.lineage.userId

service.runtime Details.context.targetProcess.lineage.uuid

service.runtime Details.context.targetProcess.name

service.runtime Details.context.targetProcess.namespacePid

service.runtime Details.context.targetProcess.parentUuid

service.runtime Details.context.targetProcess.pid

service.runtime Details.context.targetProcess.pwd

service.runtime Details.context.targetProcess.startTime

service.runtime Details.context.targetProcess.user

service.runtime Details.context.targetProcess.userId

service.runtime Details.context.targetProcess.uuid

Nom de champ JSON

service.runtime Details.context.threatFilePath

service.runtime Details.context.toolCategory

service.runtime Details.context.toolName

service.runtime Details.process.euid

service.runtime Details.process.lineage.euid

service.runtime Details.process.lineage.executablePath

service.runtime Details.process.lineage.name

service.runtime Details.process.lineage.namespacePid

service.runtime Details.process.lineage.parentUid

service.runtime Details.process.lineage.pid

service.runtime Details.process.lineage.startTime

service.runtime Details.process.lineage.userId

service.runtime Details.process.lineage.uuid

service.runtime Details.process.namespacePid

service.runtime Details.process.parentUid

service.runtime Details.process.pid

service.runtime Details.process.pwd

service.runtime Details.process.startTime

service.runtime Details.process.user

service.runtime Details.process.userId

Nom de champ JSON

service.runtime Details.process.uuid

Service. Commentaires des utilisateurs

Règles de suppression dans GuardDuty

Une règle de suppression est un ensemble de critères, composés d'un attribut de filtre associé à une valeur, utilisés pour filtrer les résultats en archivant automatiquement les nouveaux résultats qui correspondent aux critères spécifiés. Les règles de suppression peuvent être utilisées pour filtrer les résultats de faible valeur, les faux positifs ou les menaces sur lesquelles vous n'avez pas l'intention d'agir. Cela facilite la reconnaissance des menaces de sécurité ayant le plus d'impact sur votre environnement.

Après avoir créé une règle de suppression, les nouveaux résultats qui correspondent aux critères définis dans la règle sont automatiquement archivés tant que la règle de suppression est active. Vous pouvez utiliser un filtre existant pour créer une règle de suppression ou créer une règle de suppression à partir d'un nouveau filtre que vous définissez. Vous pouvez configurer des règles de suppression pour supprimer des types de recherche entiers ou définir des critères de filtre plus précis afin de supprimer uniquement des instances spécifiques d'un type de résultat particulier. Vous pouvez modifier les règles de suppression à tout moment.

Les résultats supprimés ne sont pas envoyés à AWS Security Hub CSPM Amazon Simple Storage Service, Amazon Detective ou Amazon EventBridge, ce qui réduit le niveau de bruit lié à la recherche si vous utilisez GuardDuty les résultats via Security Hub CSPM, un SIEM tiers ou d'autres applications d'alerte et de billetterie. Si vous l'avez activée [Protection contre les logiciels malveillants pour EC2](#), les GuardDuty résultats supprimés ne lanceront pas d'analyse des programmes malveillants.

GuardDuty continue de générer des résultats même s'ils correspondent à vos règles de suppression, mais ces résultats sont automatiquement marqués comme archivés. Les résultats archivés sont conservés GuardDuty pendant 90 jours et peuvent être consultés à tout moment pendant cette période. Vous pouvez consulter les résultats supprimés dans la GuardDuty console en sélectionnant Archivé dans le tableau des résultats, ou via l' GuardDuty API en utilisant l'[ListFindings](#) API avec un `findingCriteria` critère `service.archived` égal à vrai.

 Note

Dans un environnement multi-comptes, seul l' GuardDuty administrateur peut créer des règles de suppression.

Utilisation des règles de suppression avec la détection étendue des menaces

GuardDuty Extended Threat Detection détecte automatiquement les attaques en plusieurs étapes qui couvrent des sources de données, plusieurs types de AWS ressources et des délais, au cours d'une Compte AWS seule opération. Il met en corrélation les événements provenant de différentes sources de données afin d'identifier les scénarios qui se présentent comme une menace potentielle pour votre AWS environnement, puis génère une recherche de séquence d'attaque. Pour de plus amples informations, veuillez consulter [Comment fonctionne la détection étendue des menaces](#).

Lorsque vous créez des règles de suppression qui archivent les résultats, Extended Threat Detection ne peut pas utiliser ces résultats archivés pour corréler les événements des séquences d'attaques. Des règles de suppression étendues peuvent avoir un impact sur la capacité GuardDuty à détecter des comportements liés à la détection d'attaques en plusieurs étapes. Les résultats archivés en raison des règles de suppression ne sont pas considérés comme des signaux pour les séquences d'attaque. Par exemple, si vous créez une règle de suppression qui archive tous les résultats liés au cluster EKS au lieu de cibler des activités connues spécifiques, vous GuardDuty ne pourrez pas utiliser ces résultats pour détecter une séquence d'attaque dans laquelle un acteur de la menace exploite un conteneur, obtient des jetons privilégiés et accède à des ressources sensibles.

Tenez compte des recommandations suivantes émanant de GuardDuty :

- Continuez à utiliser les règles de suppression pour réduire les alertes provenant d'activités fiables connues.
- Veillez à ce que les règles de suppression se concentrent sur les comportements spécifiques pour lesquels vous ne GuardDuty souhaitez pas générer de résultat.

Cas d'utilisation courants des règles de suppression et exemples

Les types de résultats suivants présentent des cas d'utilisation courants pour appliquer des règles de suppression. Sélectionnez le nom de la découverte pour en savoir plus sur cette découverte.

Consultez la description du cas d'utilisation pour décider si vous souhaitez créer une règle de suppression pour ce type de recherche.

 Important

GuardDuty vous recommande de créer des règles de suppression de manière réactive et uniquement pour les résultats pour lesquels vous avez identifié à plusieurs reprises des faux positifs dans votre environnement.

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#) : utilisez une règle de suppression pour archiver automatiquement les résultats générés lorsque la mise en réseau de VPC est configurée de manière à acheminer le trafic Internet pour qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet de VPC.

Ce résultat est généré lorsque la mise en réseau est configurée pour acheminer le trafic Internet de telle sorte qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet VPC (IGW). Les configurations courantes, telles que [AWS Outposts](#) ou les connexions VPN VPC, peuvent entraîner l'acheminement du trafic de cette façon. Si ce comportement est normal, il est recommandé d'utiliser des règles de suppression et de créer une règle composée de deux critères de filtre. Le premier critère est le type de résultat, qui devrait être `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Le deuxième critère de filtre est l'adresse IPv4 de l'appelant d'API avec l'adresse IP ou la plage d'adresses CIDR de votre passerelle Internet sur site. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction de l'adresse IP de l'appelant d'API.

Finding type: `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`
API caller IPv4 address: `198.51.100.6`

 Note

Pour inclure plusieurs adresses IP d'appelants d'API, vous pouvez ajouter chaque adresse IP à la liste de valeurs pour Equals ou NotEquals conditions, ou utiliser des modèles génériques pour les correspondances ou NotMatches les conditions. Une NotEquals valeur égale ou égale peut également être une plage d'adresses CIDR, qui correspond à n'importe quelle adresse IP comprise dans cette plage.

- [Recon:EC2/Portscan](#) : utilisez une règle de suppression pour archiver automatiquement les résultats lors de l'utilisation d'une application d'évaluation des vulnérabilités.

La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur Recon:EC2/Portscan. Le second critère de filtre doit correspondre à l'instance ou aux instances qui hébergent ces outils d'évaluation de vulnérabilité. Vous pouvez utiliser l'attribut ID d'image d'instance ou Valeur de balise en fonction des critères identifiables avec les instances qui hébergent ces outils. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction des instances avec une certaine AMI.

Finding type: *Recon:EC2/Portscan* Instance image ID: *ami-999999999*

- [UnauthorizedAccess:EC2/SSHBruteForce](#) : utilisez une règle de suppression pour archiver automatiquement les résultats lorsque la règle est ciblée sur des instances de bastion.

Si la cible de la tentative de force brute est un hôte bastion, cela peut correspondre au comportement attendu de votre AWS environnement. Dans ce cas, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur UnauthorizedAccess:EC2/SSHBruteForce. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction des instances avec une certaine valeur de balise d'instance.

Finding type: *UnauthorizedAccess:EC2/SSHBruteForce* Instance tag value: *devops*

- [Recon:EC2/PortProbeUnprotectedPort](#) : utilisez une règle de suppression pour archiver automatiquement les résultats lorsque la règle est ciblée sur des instances exposées intentionnellement.

Dans certains cas, les instances peuvent être intentionnellement exposées, par exemple si elles hébergent des serveurs Web. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur Recon:EC2/PortProbeUnprotectedPort. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image

d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction des instances avec une certaine clé de balise d'instance dans la console.

Finding type: *Recon:EC2/PortProbeUnprotectedPort* Instance tag key: *prod*

Règles de suppression recommandées pour les résultats de Runtime Monitoring

- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#) est généré lorsqu'un processus à l'intérieur d'un conteneur communique avec le socket Docker. Certains conteneurs de votre environnement peuvent avoir besoin d'accéder au socket Docker pour des raisons légitimes. L'accès à partir de tels conteneurs générera un résultat PrivilegeEscalation:Runtime/DockerSocketAccessed. Si tel est le cas dans votre AWS environnement, nous vous recommandons de configurer une règle de suppression pour ce type de détection. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur PrivilegeEscalation:Runtime/DockerSocketAccessed. Le deuxième critère de filtre est le champ Chemin exécutable dont la valeur est égale à celle du executablePath du processus dans le résultat généré. Alternativement, le second critère de filtre peut utiliser un SHA-256 champ exécutable dont la valeur est égale à celle du processus executableSha256 dans le résultat généré.
- Les clusters Kubernetes exécutent leurs propres serveurs DNS en tant que pods, comme coredns. Par conséquent, pour chaque recherche DNS à partir d'un espace, GuardDuty capture deux événements DNS, l'un provenant de l'espace et l'autre du module serveur. Cela peut générer des doublons pour les résultats DNS suivants :
 - [Backdoor:Runtime/C&A;Activity.B! DNS](#)
 - [CryptoCurrency:Runtime/BitcoinTool.B! DNS](#)
 - [Impact:Runtime/AbusedDomainRequest.Reputation](#)
 - [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
 - [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
 - [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
 - [Trojan:Runtime/BlackholeTraffic! DNS](#)
 - [Trojan:Runtime/DGADomainRequest.C! DNS](#)
 - [Trojan:Runtime/DriveBySourceTraffic! DNS](#)
 - [Trojan:Runtime/DropPoint! DNS](#)

- [Trojan:Runtime/PhishingDomainRequest! DNS](#)

Les résultats en double incluront les détails du pod, du conteneur et du processus correspondant à votre pod de serveur DNS. Vous pouvez définir une règle de suppression pour supprimer ces résultats en double à l'aide de ces champs. Le premier critère de filtre doit utiliser le champ Type de résultat avec une valeur égale à un type de résultat DNS figurant dans la liste des résultats fournie plus haut dans cette section. Le deuxième critère de filtre peut être soit un chemin exécutable dont la valeur est égale à celle de votre serveur DNS, `executablePath` soit un exécutable SHA-256 dont la valeur est égale à celle de votre serveur DNS `executableSHA256` dans le résultat généré. En tant que troisième critère de filtre facultatif, vous pouvez utiliser le champ Image de conteneur Kubernetes avec une valeur égale à l'image de conteneur de votre pod de serveur DNS dans le résultat généré.

Création de règles de suppression dans GuardDuty

Une règle de suppression est un ensemble de critères qui inclut l'utilisation d'attributs de filtre et la fourniture de valeurs pour lesquelles vous ne souhaitez pas que GuardDuty génère de type de recherche. Les types de résultats correspondant à ces critères sont automatiquement archivés. Pour réduire le bruit, les résultats supprimés ne sont envoyés à aucun Services AWS des sites que vous pourriez intégrer. Pour plus d'informations sur les cas d'utilisation courants liés à la création de règles de suppression, consultez [Règles de suppression](#).

Vous pouvez visualiser, créer et gérer les règles de suppression à l'aide de la page Règles de suppression de la GuardDuty console. Les règles de suppression peuvent également être générées à partir de vos filtres enregistrés existants. Pour plus d'informations sur la création de filtres, veuillez consulter [Filtrer les résultats dans GuardDuty](#).

Les critères de filtre peuvent inclure une correspondance exacte à l'aide de `Equals` et `NotEquals` opérateurs, une correspondance générique à l'aide des `Correspondances` et des `NotMatches` opérateurs ou une correspondance de comparaison à l'aide des `LessThanEquals` opérateurs `GreaterThan` `GreaterThanEquals`, `LessThan` et. Vous trouverez plus d'informations sur les opérateurs disponibles [Conditions](#) sur cette page.

Choisissez votre méthode d'accès préférée pour créer une règle de suppression permettant de GuardDuty rechercher des types.

Console

Pour créer une règle de suppression à l'aide de la console :

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Sur la page Règles de suppression, cliquez sur Créer une règle de suppression pour ouvrir le formulaire Créer une règle de suppression.
3. Entrez un nom pour la règle de suppression. Le nom doit être composé de 3 à 64 caractères. Les caractères valides sont les suivants : a-z A-Z, 0-9, point (.), tiret (-) et trait de soulignement (_).
4. La description est facultative. Si vous saisissez une description, celle-ci peut comporter jusqu'à 512 caractères. Les caractères valides sont les suivants : a-z A-Z, 0-9, point (.), tiret (-), deux-points (:), crochets ({ } () []), barre oblique (/) et espace.
5. Le rang est facultatif. Il peut s'agir d'une valeur numérique comprise entre 1 et le nombre total de filtres et de règles de suppression, plus 1.
6. Dans la section Attributs, sélectionnez une clé et un opérateur dans la liste déroulante.
7. Entrez la valeur « chaîne » ou « date » dans le sélecteur de date en fonction de la clé sélectionnée. S'il s'agit d'une valeur de chaîne, saisissez le texte et appuyez sur Entrée. Plusieurs valeurs peuvent être ajoutées en cas de valeurs de chaîne.
8. Des critères supplémentaires peuvent être ajoutés en sélectionnant Ajouter des critères pour ajouter un autre ensemble de clés, d'opérateurs et de valeurs.
9. Sélectionnez Créer une règle de suppression pour créer et enregistrer la règle de suppression.

Vous pouvez également créer une règle de suppression à partir d'un filtre enregistré existant. Pour plus d'informations sur la création de filtres, veuillez consulter [Filtrer les résultats dans GuardDuty](#).

Pour créer une règle de suppression à partir d'un filtre enregistré :

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Sur la page Résultats, dans le menu Règles enregistrées, sélectionnez une règle de jeu de filtres enregistrée. Cela affichera automatiquement l'ensemble de filtres et les résultats correspondant aux critères.

3. Vous pouvez également ajouter d'autres critères de filtre à cette règle enregistrée. Si vous n'avez pas besoin de critères de filtre supplémentaires, ignorez cette étape. Pour ajouter un ou plusieurs critères de filtre, suivez les étapes 3 à 7 de la section [Adding filters on Findings page](#), puis passez aux étapes suivantes.
4. Après avoir ajouté les critères de filtrage et confirmé que les résultats filtrés répondent à vos exigences, choisissez **Créer une règle de suppression**.
5. Entrez un nom pour la règle de suppression. Le nom doit être composé de 3 à 64 caractères. Les caractères valides sont les suivants : a-z A-Z, 0-9, point (.), tiret (-) et trait de soulignement (_).
6. La description est facultative. Si vous saisissez une description, celle-ci peut comporter jusqu'à 512 caractères.
7. Choisissez **Créer**.
8. Si vous n'avez pas besoin d'ajouter des critères de filtre supplémentaires à la règle enregistrée, suivez les étapes 4 à 7 pour créer le filtre.

API/CLI

Pour créer une règle de suppression à l'aide de l'API :

1. Vous pouvez créer des règles de suppression via l'API [CreateFilter](#). Pour ce faire, spécifiez les critères de filtre dans un fichier JSON en suivant le format de l'exemple détaillé ci-dessous. L'exemple ci-dessous supprimera tous les résultats non archivés de faible gravité contenant une requête DNS adressée au `test.example.com` domaine. Pour les résultats de gravité moyenne, la liste d'entrée sera `["4", "5", "7"]`. Pour les résultats de gravité élevée, la liste d'entrée sera `["6", "7", "8"]`. Pour les résultats de gravité critique, la liste d'entrée sera `["9", "10"]`. Vous pouvez également filtrer en fonction de n'importe quelle valeur de la liste.

L'exemple suivant ajoute un filtre pour les résultats de faible gravité pour les fonctions lambda dont le nom de fonction est le préfixe « `MyFunc` » et la balise de fonction dont le préfixe n'est pas « » `TestTag`

```
{
  "Criterion": {
    "service.action.dnsRequestAction.domain": {
      "Equals": [
```

```

        "test.example.com"
    ]
},
"severity": {
    "Equals": [
        "1",
        "2",
        "3"
    ]
}
}
}

```

Vous pouvez créer des règles de suppression à l'aide de caractères génériques * et ? . Les caractères génériques dans les filtres sont pris en charge à l'aide des correspondances et des NotMatches opérateurs uniquement. Pour faire correspondre un nombre quelconque de caractères, vous pouvez utiliser * dans la valeur de l'attribut et pour faire correspondre un seul caractère, vous pouvez utiliser ? dans la valeur de l'attribut. Les filtres prennent en charge un maximum de 5 attributs sous une seule condition de caractère générique et un maximum de 5 caractères génériques dans un seul attribut. L'exemple suivant ajoute un filtre pour le nom Lambda correspondant au préfixe « MyFunc », mais pas pour les fonctions Lambda dont les balises ont pour préfixe « TestTag », suivi de 0 à 2 caractères.

```

{
  "Criterion": {
    "resource.lambdaDetails.functionName": {
      "Matches": [
        "MyFunc*"
      ]
    },
    "resource.lambdaDetails.tags.key": {
      "NotMatches": [
        "TestTag??"
      ]
    }
  }
}

```

Pour obtenir la liste des noms de champ JSON et leur équivalent dans la console, veuillez consulter [Filtres de propriétés dans GuardDuty](#).

Pour tester vos critères de filtre, utilisez le même critère JSON dans l'API [ListFindings](#) et vérifiez que les résultats corrects ont été sélectionnés. Pour tester vos critères de filtre, AWS CLI suivez l'exemple en utilisant votre propre DetectorID et votre fichier .json.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#)API.

```
aws guardduty list-detector
```

```
aws guardduty list-findings \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--finding-criteria file://criteria.json
```

Note

La correspondance des caractères génériques n'est pas disponible pour ListFindings et GetFindingsStatistics Les critères contenant des caractères génériques ne peuvent pas être validés à l'aide de ListFindings et GetFindingsStatistics.

2. Téléchargez votre filtre à utiliser en tant que règle de suppression avec l'API [CreateFilter](#) ou via l'interface de ligne de commande AWS en suivant l'exemple ci-dessous avec votre ID de détecteur, un nom pour la règle de suppression et votre fichier .json.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#)API.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  

```



```
--action ARCHIVE \  
--name yourfiltername \  
--finding-criteria file://criteria.json
```

Vous pouvez consulter la liste de vos filtres par programmation à l'aide de l'API [ListFilter](#). Vous pouvez consulter les détails d'un filtre individuel en fournissant le nom du filtre à l'API [GetFilter](#). Mettez à jour les filtres à l'aide de [UpdateFilter](#) ou supprimez-les avec l'API [DeleteFilter](#).

Mise à jour des règles de suppression dans GuardDuty

Cette section décrit les étapes à suivre pour mettre à jour une règle de suppression Compte AWS dans votre environnement spécifique Région AWS.

Vous pouvez mettre à jour les règles de suppression existantes depuis la page Règles de suppression de la GuardDuty console. GuardDuty prend en charge la mise à jour de la description, du classement et des critères de filtrage du filtre de suppression depuis la GuardDuty console ou à l'aide du GuardDuty CLI/API. La mise à jour de la règle de suppression suit les mêmes restrictions sur les valeurs des champs pour la description, le rang et les critères que [Création de règles de suppression](#).

Si vous êtes un compte membre, votre compte administrateur peut effectuer cette action en votre nom. Pour de plus amples informations, veuillez consulter [Relations entre le compte administrateur et le compte membre](#).

Choisissez votre méthode d'accès préférée pour supprimer une règle de suppression pour GuardDuty findingtypes.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Sur la page Règles de suppression, sélectionnez la règle de suppression à mettre à jour.
3. Dans la liste déroulante Actions, sélectionnez Mettre à jour la règle de suppression.
4. Cela ouvre le formulaire de règle de suppression existant.
5. Apportez les modifications nécessaires à la section Description, classement et attributs.
6. Sélectionnez Mettre à jour la règle de suppression pour mettre à jour la règle de suppression.

API/CLI

Pour mettre à jour une règle de suppression à l'aide de l'API :

1. Vous pouvez mettre à jour les règles de suppression via l' UpdateFilter API. Seuls la description, le classement et les critères peuvent être mis à jour à l'aide de l' UpdateFilter API. Ces trois champs sont facultatifs.
2. Pour mettre à jour un filtre existant, vous aurez besoin du nom du filtre que vous souhaitez mettre à jour.
3. Si vous souhaitez mettre à jour les critères existants, créez un fichier JSON contenant les critères mis à jour, de la même manière que vous avez créé le filtre pour la première fois. Exemple de critère permettant de supprimer tout résultat non archivé de faible gravité contenant une requête DNS adressée au domaine test.example.com. Pour les résultats de gravité moyenne, la liste d'entrée sera ["4", « 5", « 7"]. Pour les résultats de gravité élevée, la liste d'entrée sera ["6", « 7", « 8"]. Pour les résultats de gravité critique, la liste d'entrée sera ["9", « 10"]. Vous pouvez également filtrer en fonction de n'importe quelle valeur de la liste. L'exemple suivant ajoute un filtre pour les résultats de faible gravité.

```
{
  "Criterion": {
    "service.action.dnsRequestAction.domain": {
      "Equals": [
        "test.example.com"
      ]
    },
    "severity": {
      "Equals": [
        "1",
        "2",
        "3"
      ]
    }
  }
}
```

Pour obtenir la liste des noms de champ JSON et leur équivalent dans la console, veuillez consulter [Filtres de propriétés dans GuardDuty](#).

Pour tester vos critères de filtre, utilisez le même critère JSON dans l'API [ListFindings](#) et vérifiez que les résultats corrects ont été sélectionnés. Pour tester vos critères de filtre, AWS CLI suivez l'exemple en utilisant votre propre DetectorID et votre fichier .json.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

```
aws guardduty list-detectors --region us-east-1
```

4. Si vous souhaitez mettre à jour la description, vous pouvez inclure le paramètre de description dans l'appel CLI.
5. Si vous souhaitez mettre à jour le classement, vous pouvez inclure le paramètre de classement dans l'appel CLI.
6. Si vous souhaitez passer d'un filtre de suppression à un filtre normal, utilisez le paramètre d'action et la valeur `ARCHIVE` dans l'appel CLI.
7. Mettez à jour votre API de filtrage existante ou utilisez l' AWS CLI exemple ci-dessous avec votre propre identifiant de détecteur, un nom pour la règle de suppression et un fichier .json.
8. Voici un exemple de CLI qui met à jour tous les paramètres décrits ci-dessus. Vous pouvez sélectionner les paramètres spécifiques à mettre à jour pour votre cas d'utilisation à l'aide de la commande -

```
aws guardduty update-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--action ARCHIVE \  
--rank 1 \  
--description "Updated description" \  
--finding-criteria file://criteria.json
```

Supprimer les règles de suppression dans GuardDuty

Cette section décrit les étapes à suivre pour supprimer une règle de suppression Compte AWS dans votre compte Région AWS.

Vous souhaitez peut-être supprimer une règle de suppression qui ne décrit plus le comportement attendu dans votre environnement. Vous ne souhaitez plus supprimer le type de recherche associé afin de GuardDuty pouvoir générer un type de recherche.

Si vous êtes un compte membre, votre compte administrateur peut effectuer cette action en votre nom. Pour de plus amples informations, veuillez consulter [Relations entre le compte administrateur et le compte membre](#).

Choisissez votre méthode d'accès préférée pour supprimer une règle de suppression permettant de GuardDuty rechercher des types.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Sur la page Règles de suppression, sélectionnez la règle de suppression à supprimer.
3. Dans la liste déroulante Actions, sélectionnez Supprimer la règle de suppression.
4. Une fenêtre de confirmation s'affiche. Sélectionnez Supprimer pour poursuivre la suppression. Ou sélectionnez Annuler pour annuler l'opération.

API/CLI

Exécutez l'API [DeleteFilter](#). Spécifiez le nom du filtre et l'ID de détecteur associé pour la région en question.

Vous pouvez également utiliser l' AWS CLI exemple suivant en remplaçant les valeurs formatées dans *red* :

```
aws guardduty delete-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--filter-name filterName \  
--region us-east-1
```

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

Métriques relatives aux règles de suppression

Amazon vous permet GuardDuty de contrôler la fréquence à laquelle chaque règle de suppression correspond et d'archiver les résultats. GuardDuty publie ces métriques sur Amazon CloudWatch sous l'espace de AWS/GuardDuty noms.

 GuardDuty les nombres correspondaient aux résultats et supprimaient les résultats différemment

GuardDuty émet FindingsMatchedByFilter lorsqu'un résultat correspond à une règle de suppression ou à un filtre NOOP (filtre sans action). Cette métrique augmente quelle que soit l'action du filtre. GuardDuty n'est émis FindingsSuppressedByFilter que lorsque l'action de la règle est Archiver et que la règle est la règle d'archivage la plus prioritaire pour cette découverte.

GuardDuty publie les statistiques des règles de suppression en fonction de la configuration de votre compte :

- Pour les comptes autonomes (ne faisant pas partie d'une organisation), GuardDuty publie les statistiques sur ce compte.
- Pour les comptes faisant partie d'une organisation, GuardDuty publie les statistiques sur le compte d'administrateur délégué. Pour plus d'informations sur le fonctionnement des comptes d'administrateur et de membre GuardDuty, consultez [Gérer plusieurs comptes sur Amazon GuardDuty](#).

Détails du système métrique

Le tableau suivant décrit les CloudWatch métriques Amazon GuardDuty publiées pour les règles de suppression.

Métrique	Unité	Description
FindingsMatchedByFilter	Nombre	Nombre de résultats correspondant aux critères d'une règle de suppression ou d'un filtre NOOP. Un résultat peut correspondre à plusieurs règles de suppression ou filtres NOOP, et il est GuardDuty comptabilisé une fois par correspondance. Chaque match génère 1 point de données.
FindingsSuppressedByFilter	Nombre	Nombre de résultats archivés par une règle de suppression. Lorsque plusieurs règles correspondent au même résultat, seule la règle dont la Rank valeur est la plus faible est prise en GuardDuty compte. Chaque suppression génère 1 point de données.

Afficher les statistiques des règles de suppression sur Amazon CloudWatch

Vous trouverez les métriques des règles de suppression dans la CloudWatch console Amazon sous l'espace de `AWS/GuardDuty` noms, regroupées par `FilterName` dimension. La valeur de la `FilterName` dimension est le nom de la règle ou du filtre de suppression. Pour obtenir des instructions sur la localisation et la représentation graphique des métriques sur Amazon CloudWatch, consultez la section [Affichage des métriques disponibles](#) dans le guide de CloudWatch l'utilisateur Amazon.

Personnalisation de la détection des menaces à l'aide de listes d'entités et de listes d'adresses IP

Amazon GuardDuty surveille la sécurité de votre AWS environnement en analysant et en traitant les journaux de flux VPC, les journaux d' AWS CloudTrail événements et les journaux DNS. En activant un ou plusieurs [plans de GuardDuty protection Use-case ciblés](#) (sauf [Surveillance d'exécution](#)), vous pouvez étendre les fonctionnalités de surveillance qu'ils contiennent GuardDuty.

Grâce aux listes, GuardDuty vous pouvez personnaliser l'étendue de la détection des menaces dans votre environnement. Vous pouvez configurer GuardDuty pour arrêter de générer des résultats à partir de vos sources fiables et générer des résultats pour des sources malveillantes connues à partir de vos listes de menaces. GuardDuty continue de prendre en charge les anciennes listes d'adresses IP et étend la prise en charge aux listes d'entités (recommandé) qui peuvent contenir des adresses IP, des domaines ou les deux.

Rubriques

- [Comprendre les listes d'entités et les listes d'adresses IP](#)
- [Considérations importantes relatives aux GuardDuty listes](#)
- [Formats de liste](#)
- [Comprendre les statuts des listes](#)
- [Configuration des prérequis pour les listes d'entités et les listes d'adresses IP](#)
- [Ajouter et activer une liste d'entités ou une liste d'adresses IP](#)
- [Mettre à jour une liste d'entités ou une liste d'adresses IP](#)
- [De-activating liste d'entités ou liste d'adresses IP](#)
- [Supprimer une liste d'entités ou une liste d'adresses IP](#)

Comprendre les listes d'entités et les listes d'adresses IP

GuardDuty propose deux approches de mise en œuvre : les listes d'entités (recommandées) et les listes d'adresses IP. Les deux approches vous aident à définir les sources fiables, qui cessent GuardDuty de générer des découvertes, et les menaces connues, qui sont GuardDuty utilisées pour générer des conclusions.

Les listes d'entités prennent en charge les adresses IP, les noms de domaine et les hachages de SHA-256 fichiers. Ils utilisent un accès direct à Amazon Simple Storage Service (Amazon S3) avec

une seule autorisation IAM qui n'a aucune incidence sur les limites de taille des politiques IAM dans plusieurs régions.

Les listes IP ne prennent en charge que les adresses IP et leur utilisation [GuardDuty rôle lié à un service \(SLR\)](#) (SLR), ce qui nécessite des mises à jour des politiques IAM par région, ce qui peut avoir une incidence sur les limites de taille des politiques IAM.

Les listes fiables (listes d'entités et listes d'adresses IP) incluent des entrées auxquelles vous faites confiance pour une communication sécurisée avec votre AWS infrastructure. GuardDuty ne génère pas de résultats pour les entrées répertoriées dans des sources fiables. À tout moment, vous ne pouvez ajouter qu'une seule liste d'entités de confiance et une seule liste d'adresses IP de confiance Compte AWS par région.

Les listes de menaces (listes d'entités et listes d'adresses IP) incluent des entrées que vous avez identifiées comme des sources malveillantes connues. Lorsqu'il GuardDuty détecte une activité impliquant ces sources, il génère des résultats pour vous avertir de problèmes de sécurité potentiels. Vous pouvez créer vos propres listes de menaces ou intégrer des flux de renseignements tiers sur les menaces. Cette liste peut être fournie par des renseignements tiers sur les menaces ou créée spécifiquement pour votre organisation. En plus de générer des résultats en raison d'une activité potentiellement suspecte, il génère GuardDuty également des résultats basés sur une activité impliquant des entrées de vos listes de menaces. À tout moment, vous pouvez télécharger jusqu'à six listes d'entités menaçantes et listes d'adresses IP de menaces Compte AWS par région.

Note

Pour migrer des listes d'adresses IP vers les listes d'entités [Conditions requises pour les listes d'entités](#), suivez, puis ajoutez et activez la liste d'entités requise. Ensuite, vous pouvez choisir de désactiver ou de supprimer la liste d'adresses IP correspondante.

Considérations importantes relatives aux GuardDuty listes

Avant de commencer à travailler avec des listes, prenez connaissance des points suivants :

- Les listes d'adresses IP et les listes d'entités s'appliquent uniquement au trafic destiné aux adresses IP et aux domaines routables publiquement.
- Dans une liste d'entités, les entrées s'appliquent aux CloudTrail journaux de flux VPC dans Amazon VPC et aux résultats des journaux de requêtes DNS de Route53 Resolver.

Dans une liste d'adresses IP, les entrées s'appliquent aux CloudTrail journaux de flux VPC contenus dans les résultats d'Amazon VPC, mais pas aux résultats des journaux de requêtes DNS de Route53 Resolver.

- Si vous incluez la même adresse IP ou le même domaine à la fois dans les listes de confiance et de menaces, cette entrée de la liste de confiance aura la priorité. GuardDuty ne générera pas de résultat s'il existe une activité associée à cette entrée.
- Dans un environnement multi-comptes, seul le compte GuardDuty administrateur peut gérer les listes. Ce paramètre s'applique automatiquement aux comptes des membres. GuardDuty génère des résultats basés sur une activité impliquant des adresses IP (et des domaines) malveillants connus provenant des sources de menace du compte administrateur, et ne génère pas de résultats basés sur une activité impliquant des adresses IP (et des domaines) provenant des sources fiables du compte administrateur. Pour de plus amples informations, veuillez consulter [Gérer plusieurs comptes sur Amazon GuardDuty](#).
- Seules les adresses IPv4 sont acceptées. Les adresses IPv6 ne sont pas prises en charge.
- SHA-256 les hachages de fichiers ne sont pris en charge que dans les listes d'entités de menace. Vous ne pouvez pas inclure les hachages de fichiers dans les listes d'entités fiables ou les listes d'adresses IP.
- Une fois que vous avez activé, désactivé ou supprimé une liste d'entités ou une liste d'adresses IP, le processus devrait être terminé dans les 15 minutes. Dans certains scénarios, l'exécution de ce processus peut prendre jusqu'à 40 minutes.
- GuardDuty utilise une liste pour détecter les menaces uniquement lorsque le statut de la liste devient Actif.
- Chaque fois que vous ajoutez ou mettez à jour une entrée dans l'emplacement du compartiment S3 de la liste, vous devez réactiver la liste. Pour de plus amples informations, veuillez consulter [Mettre à jour une liste d'entités ou une liste d'adresses IP](#).
- Les listes d'entités et les adresses IP ont des quotas différents. Pour de plus amples informations, veuillez consulter [GuardDuty quotas](#).

Formats de liste

GuardDuty accepte plusieurs formats de fichier pour vos listes et listes d'entités, avec un maximum de 35 Mo par fichier. Chaque format a des exigences et des fonctionnalités spécifiques.

Texte brut (TXT)

Ce format prend en charge les adresses IP, les plages d'adresses CIDR, les noms de domaine et les hachages de SHA-256 fichiers. SHA-256 les hachages de fichiers ne sont pris en charge que dans les listes d'entités de menace. Chaque entrée doit apparaître sur une ligne distincte.

Exemple Exemple de liste d'entités

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
```

Exemple Exemple de liste d'entités menaçantes avec hachage de fichiers

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

Exemple Exemple de liste d'adresses IP

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

Structured Threat Information Expression (STIX)

Ce format prend en charge les adresses IP, les blocs CIDR, les noms de domaine et les hachages de SHA-256 fichiers. STIX vous permet d'inclure un contexte supplémentaire dans vos informations sur les menaces. GuardDuty traite les adresses IP, les plages d'adresses CIDR, les noms de domaine et les hachages de SHA-256 fichiers à partir des indicateurs STIX. SHA-256 les hachages de fichiers ne sont pris en charge que dans les listes d'entités de menace.

Exemple Exemple de liste d'entités

```
<?xml version="1.0" encoding="UTF-8"?>
```

```

<stix:STIX_Package
  xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
  id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
  version="1.2">
  <stix:Indicators>
    <stix:Indicator
      id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
      timestamp="2025-08-12T00:00:00Z"
      xsi:type="indicator:IndicatorType"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <indicator:Title>Malicious domain observed Example</indicator:Title>
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
Watchlist</indicator:Type>
      <indicator:Observable id="example:Observable-0000-1111-2222-3333">
        <cybox:Object id="example:Object-0000-1111-2222-3333">
          <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
            <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
          </cybox:Properties>
        </cybox:Object>
      </indicator:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>

```

Exemple Exemple de liste d'entités menaçantes avec hachage de fichiers

```

<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
  xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"

```

```

xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
version="1.2">
<stix:Indicators>
  <stix:Indicator
    id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeefffff"
    timestamp="2025-08-12T00:00:00Z"
    xsi:type="indicator:IndicatorType"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <indicator:Title>Malicious domain observed Example</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
Watchlist</indicator:Type>
    <indicator:Observable id="example:Observable-0000-1111-2222-3333">
      <cybox:Object id="example:Object-0000-1111-2222-3333">
        <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
          <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
  </stix:Indicator>
  <stix:Indicator
    id="example:indicator-a1b2c3d4-eeee-ffff-0000-111122223333"
    timestamp="2025-08-12T00:00:00Z"
    xsi:type="indicator:IndicatorType"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <indicator:Title>File hash for malware variant</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
Watchlist</indicator:Type>
    <indicator:Observable id="example:Observable-4444-5555-6666-7777">
      <cybox:Object id="example:File-4444-5555-6666-7777">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
          <FileObj:Hashes>
            <cyboxCommon:Hash>
              <cyboxCommon:Type
xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value
condition="Equals">a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3</
cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
          </FileObj:Hashes>
        </cybox:Properties>
      </cybox:Object>

```

```

        </indicator:Observable>
    </stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>

```

Exemple Exemple de liste d'adresses IP

```

<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:ttp="http://stix.mitre.org/TTP-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
    stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
    campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
    indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
    default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
    objects/Address/2.1/Address_Object.xsd"
  id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
  version="1.2">
  <stix:Observables cybox_major_version="1" cybox_minor_version="1">
    <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
      <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">

        <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
      </cybox:Properties>
    </cybox:Object>

```

```

    </cybox:Observable>
    <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
      <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
          <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
    <cybox:Observable
id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
      <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
          <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
  </stix:Observables>
</stix:STIX_Package>

```

Open Threat Exchange (OTX)TM CSV

Ce format prend en charge le bloc CIDR, les adresses IP individuelles, les domaines et le type d'indicateur pour les hachages de fichiers. SHA-256 les hachages de fichiers ne sont pris en charge que dans les listes d'entités de menace. Ce format de fichier comporte des valeurs séparées par des virgules.

Exemple Exemple de liste d'entités

```

Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example

```

Exemple Exemple de liste d'entités menaçantes avec hachage de fichiers

```

Indicator type, Indicator, Description

```

```
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
SHA256, a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, example
```

Exemple Exemple de liste d'adresses IP

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

FireEyeInformation sur les menaces™ iSight CSV

Ce format prend en charge le bloc CIDR, les adresses IP individuelles, les domaines et les hachages de SHA-256 fichiers dans la sha256 colonne. SHA-256 les hachages de fichiers ne sont pris en charge que dans les listes d'entités de menace. Les exemples de listes suivants utilisent le format FireEye™ CSV.

Exemple Exemple de liste d'entités

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
malwareFamilyId, actor, actorId, observationTime
```

[illegible]

```
01-00000002, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000002, https://www.example.com/  
report/01-00000002, , , , , , , , , , , , , , , , , , , Related,  
198.51.100.1, , , , , network, , Ursnif,  
12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , , 1494944400
```

```
01-00000003, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000003, https://www.example.com/  
report/01-00000003, , , , , , , , , , , , , , , , , Related,  
203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcf-40bc-a080-75bd35a2572d, , ,  
1494944400  
  
01-00000002, Malicious domain observed in test, Test, Operational, threat,  
1494944400, https://www.example.com/report/01-00000002,https://www.example.com/  
report/01-00000002,,,,,,,,,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,  
203.0.113.0, 8080, UDP,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,  
1494944400
```

Exemple Exemple de liste d'entités menaçantes avec hachage de fichiers

[illegible]

[illegible]

Exemple Exemple de liste d'adresses IP

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,  
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,  
recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,  
sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,  
filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,  
protocol, registrantEmail, registrantName, networkType, url, malwareFamily,  
malwareFamilyId, actor, actorId, observationTime  
  
01-000000001, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-000000001, https://www.example.com/  
report/01-000000001, , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,  
Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,  
1494944400  
  
01-000000002, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-000000002, https://www.example.com/  
report/01-000000002, , , , , , , , , , , , , , , , , , , , , , , Related,  
198.51.100.1, , , , , network, , Ursnif,  
12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400  
  
01-000000003, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-000000003, https://www.example.com/  
report/01-000000003, , , , , , , , , , , , , , , , , , , , , , , Related,  
203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcd-40bc-a080-75bd35a2572d, , ,  
1494944400
```

Proofpoint™ ET Intelligence Feed CSV

Au format ProofPoint CSV, vous pouvez ajouter des adresses IP ou des noms de domaine dans une seule liste. La liste d'exemples suivante utilise le format CSV `Proofpoint`. La fourniture d'une valeur

pour le ports paramètre est facultative. Lorsque vous ne le fournissez pas, laissez une virgule (,) à la fin.

Exemple Exemple de liste d'entités

```
domain, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

Exemple Exemple de liste d'adresses IP

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

AlienVaultFil de réputation TM

La liste d'exemples suivante utilise le format AlienVault. Ce format prend également en charge les hachages de SHA-256 fichiers dans la colonne des indicateurs. SHA-256 les hachages de fichiers ne sont pris en charge que dans les listes d'entités de menace.

Exemple Exemple de liste d'entités

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
```

Exemple Exemple de liste d'entités menaçantes avec hachage de fichiers

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3#4#2#Malicious
Hash###0.0,0.0#3
```

Exemple Exemple de liste d'adresses IP

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Comprendre les statuts des listes

Lorsque vous ajoutez une liste d'entités ou une liste d'adresses IP, GuardDuty affiche le statut de cette liste. La colonne État indique si la liste est effective et si une action est requise. La liste suivante décrit les valeurs de statut valides :

- **Actif** — Indique que la liste est actuellement utilisée pour la détection personnalisée des menaces.
- **Inactif** — Indique que la liste n'est actuellement pas utilisée. Pour utiliser cette liste GuardDuty à des fins de détection des menaces dans votre environnement, consultez Étape 3 : Activation d'une liste d'entités ou d'une liste d'adresses IP dans [Ajouter et activer une liste d'entités ou une liste d'adresses IP](#).
- **Erreur** — Indique que la liste présente un problème. Passez le curseur sur le statut pour afficher les détails de l'erreur.
- **Activation** : indique que le processus d'activation de la liste GuardDuty a été lancé. Vous pouvez continuer à surveiller le statut de cette liste. S'il n'y a pas d'erreur, le statut doit passer à Actif. Tant que le statut reste Activation, vous ne pouvez effectuer aucune action sur cette liste. Quelques minutes peuvent être nécessaires pour que le statut de la liste passe à Actif.
- **Désactivation** : indique que le processus de désactivation de la liste GuardDuty a été lancé. Vous pouvez continuer à surveiller le statut de cette liste. S'il n'y a pas d'erreur, le statut doit passer à Inactif. Tant que le statut reste Désactivation, vous ne pouvez effectuer aucune action sur cette liste.
- **Supprimer en attente** — Indique que la liste est en cours de suppression. Bien que le statut reste « Supprimer en attente », vous ne pouvez effectuer aucune action sur cette liste.

Configuration des prérequis pour les listes d'entités et les listes d'adresses IP

GuardDuty utilise des listes d'entités et des listes d'adresses IP pour personnaliser la détection des menaces dans votre AWS environnement. Les listes d'entités (recommandées) prennent en charge à la fois les adresses IP et les noms de domaine, tandis que les listes d'adresses IP ne prennent

en charge que les adresses IP. Avant de commencer à créer ces listes, vous devez ajouter les autorisations requises pour le type de liste que vous souhaitez utiliser.

Conditions requises pour les listes d'entités

Lorsque vous ajoutez des listes d'entités, GuardDuty lit vos listes de renseignements fiables et de renseignements sur les menaces à partir de compartiments S3. Le rôle que vous utilisez pour créer des listes d'entités doit disposer de `s3:GetObject` autorisation pour que les compartiments S3 contiennent ces listes.

Note

Dans un environnement multi-comptes, seul le compte GuardDuty administrateur peut gérer les listes, qui s'appliquent automatiquement aux comptes des membres.

Si vous n'avez pas encore `s3:GetObject` autorisation pour l'emplacement du compartiment S3, utilisez l'exemple de politique suivant et remplacez-le *amzn-s3-demo-bucket* par l'emplacement de votre compartiment S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
    }
  ]
}
```

Conditions requises pour les listes d'adresses IP

Les différentes identités IAM nécessitent des autorisations spéciales pour pouvoir utiliser des listes d'adresses IP fiables et des listes de menaces. GuardDuty Une identité avec la stratégie gérée [AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) attachée peut uniquement renommer et désactiver les listes d'adresses IP approuvées et les listes des menaces chargées .

Pour accorder à différentes identités un accès complet à la gestion des listes d'adresses IP approuvées et des listes des menaces (en plus de renommer et de désactiver, cela inclut l'ajout, l'activation, la suppression et la mise à jour de l'emplacement ou du nom des listes), assurez-vous que les actions suivantes sont présentes dans la stratégie d'autorisations attachée à un utilisateur, un groupe ou un rôle :

```
{
  "Effect": "Allow",
  "Action": [
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam::555555555555:role/aws-service-role/guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

Important

Ces actions ne sont pas incluses dans la politique gérée AmazonGuardDutyFullAccess.

Utilisation du SSE-KMS chiffrement avec des listes d'entités et des listes d'adresses IP

GuardDuty supports SSE-AES256 et SSE-KMS cryptage pour vos listes. SSE-C n'est pas pris en charge. Pour plus d'informations sur les types de chiffrement pour S3, consultez la section [Protection des données à l'aide du chiffrement côté serveur](#).

Que vous utilisiez des listes d'entités ou des listes d'adresses IP, si vous en utilisez SSE-KMS, ajoutez l'instruction suivante à votre AWS KMS key politique. **123456789012** Remplacez-le par votre propre identifiant de compte.

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

```
}
```

Ajouter et activer une liste d'entités ou une liste d'adresses IP

Les listes d'entités et les listes d'adresses IP vous permettent de personnaliser les fonctionnalités de détection des menaces de GuardDuty. Pour plus d'informations sur ces listes, consultez [Comprendre les listes d'entités et les listes d'adresses IP](#). Pour gérer les données fiables et les données de renseignement sur les menaces de votre AWS environnement, il est GuardDuty recommandé d'utiliser des listes d'entités. Avant de commencer, consultez [Configuration des prérequis pour les listes d'entités et les listes d'adresses IP](#).

Choisissez l'une des méthodes d'accès suivantes pour ajouter et activer une liste d'entités fiables, une liste d'entités menaçantes, une liste d'adresses IP de confiance ou une liste d'adresses IP de menaces.

Console

(Facultatif) Étape 1 : récupération de l'URL d'emplacement de votre liste

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le nom du compartiment Amazon S3 contenant la liste spécifique que vous souhaitez ajouter.
4. Choisissez le nom de l'objet (liste) pour en afficher les détails.
5. Sous l'onglet Propriétés, copiez l'URI S3 de cet objet.

Étape 2 : ajout de données fiables ou de renseignement sur les menaces

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Listes, choisissez l'onglet Listes d'entités ou Listes d'adresses IP.
4. En fonction de l'onglet que vous avez sélectionné, choisissez d'ajouter une liste de confiance ou une liste de menaces.
5. Dans la boîte de dialogue pour ajouter une liste de personnes fiables ou une liste de menaces, procédez comme suit :
 - a. Pour Nom de la liste, saisissez un nom pour votre liste.

Contraintes relatives à la dénomination de la liste : le nom de votre liste peut inclure des lettres minuscules, des majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

Pour une liste d'adresses IP, le nom de votre liste doit être unique au sein d'une région Compte AWS et.

- b. Pour Emplacement, indiquez l'emplacement où vous avez chargé votre liste. Si vous ne l'avez pas encore fait, veuillez consulter [Step 1: Fetching location URL of your list](#).

S'applique uniquement aux menaces personnalisées et aux ensembles d'entités de confiance personnalisés : si vous fournissez une URL de localisation qui ne correspond pas aux formats pris en charge suivants, vous recevrez un message d'erreur lors de l'ajout et de l'activation de la liste.

Format de l'URL de localisation :

- <https://s3.amazonaws.com/bucket.name/file.txt>
 - <https://s3-aws-region.amazonaws.com/bucket.name/file.txt>
 - <http://bucket.s3.amazonaws.com/file.txt>
 - <http://bucket.s3-aws-region.amazonaws.com/file.txt>
 - <s3://bucket.name/file.txt>
- c. (Facultatif) Pour le propriétaire attendu du compartiment, vous pouvez saisir l'ID du Compte AWS auquel appartient le compartiment Amazon S3 spécifié dans le champ Emplacement.

Lorsque vous ne spécifiez pas de propriétaire d'ID de Compte AWS, cela signifie que GuardDuty se comporte différemment pour les listes d'entités et les listes d'adresses IP. Pour les listes d'entités, GuardDuty valide que le compte du membre actuel possède le compartiment S3 spécifié dans le champ Emplacement. Pour les listes d'adresses IP, si vous ne spécifiez pas de propriétaire d'ID de Compte AWS, aucune validation GuardDuty n'est effectuée.

Si GuardDuty découvre que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de la liste.

- d. Cochez la case **J'accepte**.

- e. Choisissez Ajouter une liste. Par défaut, l'état de la liste ajoutée est Inactif. Pour que la liste soit effective, vous devez l'activer.

Étape 3 : Activation d'une liste d'entités ou d'une liste d'adresses IP

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez l'onglet dans lequel vous souhaitez activer la liste : listes d'entités ou listes d'adresses IP.
4. Sélectionnez la liste que vous souhaitez activer. Cela activera les menus Action et Edition.
5. Choisissez Action, puis sélectionnez Activer.

API/CLI

Pour ajouter et activer une liste d'entités de confiance

1. Exécutez [CreateTrustedEntitySet](#). Assurez-vous de fournir le nom `detectorId` du compte de membre pour lequel vous souhaitez créer cette liste d'entités de confiance. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

Contraintes relatives à la dénomination de la liste : le nom de votre liste peut inclure des lettres minuscules, des majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante :

```
aws guardduty create-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```


Remplacez-le `detector-id` par l'identifiant du détecteur du compte membre pour lequel vous allez créer la liste des entités de confiance, et les autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Que vous indiquiez ou non la valeur de ce paramètre, cela GuardDuty confirme que l' ID Compte AWS associé à cette `--detector-id` valeur est le propriétaire du compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

S'applique uniquement aux menaces personnalisées et aux ensembles d'entités de confiance personnalisés : si vous fournissez une URL de localisation qui ne correspond pas aux formats pris en charge suivants, vous recevrez un message d'erreur lors de l'ajout et de l'activation de la liste.

Pour ajouter et activer des listes d'entités menaçantes

1. Exécutez [CreateThreatEntitySet](#). Assurez-vous de fournir le nom `detectorId` du compte membre pour lequel vous souhaitez créer cette liste d'entités menaçantes. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

Contraintes relatives à la dénomination de la liste : le nom de votre liste peut inclure des lettres minuscules, des majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante :

```
aws guardduty create-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

Remplacez-le `detector-id` par l'identifiant du détecteur du compte membre pour lequel vous allez créer la liste des entités de confiance, et les autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Que vous indiquiez ou non la valeur de ce paramètre, cela GuardDuty confirme que l' Compte AWS ID associé à cette `--detector-id` valeur est le propriétaire du compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

S'applique uniquement aux menaces personnalisées et aux ensembles d'entités de confiance personnalisés : si vous fournissez une URL de localisation qui ne correspond pas aux formats pris en charge suivants, vous recevrez un message d'erreur lors de l'ajout et de l'activation de la liste.

Pour ajouter et activer une liste d'adresses IP fiables

1. Exécutez [CreateIPSet](#). Assurez-vous de fournir le nom `detectorId` du compte de membre pour lequel vous souhaitez créer cette liste d'adresses IP fiables. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

Pour une liste d'adresses IP, le nom de votre liste doit être unique au sein d'une région Compte AWS et.

Contraintes relatives à la dénomination de la liste : le nom de votre liste peut inclure des lettres minuscules, des majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante et en veillant à remplacer le `detector-id` par l'identifiant du détecteur du compte membre pour lequel vous allez mettre à jour la liste d'adresses IP fiables.

```
aws guardduty create-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganizationListEXAMPLE" \  

```

```
--format TXT \  
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-  
FILE.format" \  
--activate
```

Remplacez-le `detector-id` par l'identifiant du détecteur du compte membre pour lequel vous allez créer la liste d'adresses IP fiables et les autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Lorsque vous ne spécifiez pas l'ID de compte auquel appartient le compartiment S3, aucune validation GuardDuty n'est effectuée. Lorsque vous spécifiez l'ID de compte pour le `expected-bucket-owner` paramètre, cela GuardDuty confirme que cet Compte AWS ID est propriétaire du compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

Pour ajouter et activer des listes IP de menaces

1. Exécutez [CreateThreatIntelSet](#). Assurez-vous de fournir le compte `detectorId` du membre pour lequel vous souhaitez créer cette liste d'adresses IP de menaces. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectors](#) API.

Contraintes relatives à la dénomination de la liste : le nom de votre liste peut inclure des lettres minuscules, des majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

Pour une liste d'adresses IP, le nom de votre liste doit être unique au sein d'une région Compte AWS et.

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante et en veillant à remplacer le par l'`detector-id` ID du détecteur du compte membre pour lequel vous allez mettre à jour la liste des adresses IP des menaces.

```
aws guardduty create-threat-intel-set \  

```

```
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganizationListEXAMPLE" \  
--format TXT \  
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-  
FILE.format" \  
--activate
```

Remplacez-le `detector-id` par l'identifiant du détecteur du compte membre pour lequel vous allez créer la liste des adresses IP des menaces et les autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Lorsque vous ne spécifiez pas l'ID de compte auquel appartient le compartiment S3, aucune validation GuardDuty n'est effectuée. Lorsque vous spécifiez l'ID de compte pour le `expected-bucket-owner` paramètre, cela GuardDuty confirme que cet Compte AWS ID est propriétaire du compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

Après avoir activé une liste d'entités ou une liste d'adresses IP, l'efficacité de cette liste peut prendre quelques minutes. Pour de plus amples informations, veuillez consulter [Considérations importantes relatives aux GuardDuty listes](#).

Mettre à jour une liste d'entités ou une liste d'adresses IP

Les listes d'entités et les listes d'adresses IP vous aident à personnaliser les fonctionnalités de détection des menaces dans GuardDuty. Pour plus d'informations sur ces listes, consultez [Comprendre les listes d'entités et les listes d'adresses IP](#).

Vous pouvez mettre à jour le nom d'une liste, l'emplacement du compartiment S3, l'ID de compte du propriétaire attendu du compartiment et les entrées d'une liste existante. Si vous mettez à jour les entrées d'une liste, vous devez suivre les étapes pour réactiver la liste GuardDuty afin d'utiliser la dernière version de la liste. Après avoir mis à jour ou activé une liste d'entités ou une liste d'adresses IP, l'entrée en vigueur de cette liste peut prendre quelques minutes. Pour de plus amples informations, veuillez consulter [Considérations importantes relatives aux GuardDuty listes](#).

 Note

Si le statut d'une liste est Activation, Désactivation ou Supprimer en attente, vous devez attendre quelques minutes avant d'effectuer une action. Pour plus d'informations sur ces statuts, consultez [Comprendre les statuts des listes](#).

Choisissez l'une des méthodes d'accès pour mettre à jour une liste d'entités ou une liste d'adresses IP.

Console

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez l'onglet approprié : Listes d'entités ou listes d'adresses IP.
4. Sélectionnez une liste (fiable ou menaçante) que vous souhaitez mettre à jour. Cela activera le menu Action et Édition.
5. Choisissez Modifier.
6. Dans la boîte de dialogue pour mettre à jour la liste, spécifiez les détails que vous souhaitez mettre à jour.

Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

Pour une liste d'adresses IP, le nom de votre liste doit être unique au sein d'une région Compte AWS et.

S'applique uniquement aux menaces personnalisées et aux ensembles d'entités fiables personnalisés. Si vous fournissez une URL de localisation qui ne correspond pas aux formats pris en charge suivants, vous recevrez un message d'erreur lors de l'ajout et de l'activation de la liste.

7. (Facultatif) Pour le propriétaire attendu du compartiment, vous pouvez saisir l' Compte AWS ID propriétaire du compartiment Amazon S3 spécifié dans le champ Emplacement.

Lorsque vous ne spécifiez pas de propriétaire d' Compte AWS identifiant, le GuardDuty comportement est différent pour les listes d'entités et les listes d'adresses IP. Pour les listes d'entités, GuardDuty validera que le compte membre actuel possède le compartiment S3

spécifié dans le champ Emplacement. Pour les listes d'adresses IP, si vous ne spécifiez pas de propriétaire d' Compte AWS identifiant, aucune validation GuardDuty n'est effectuée.

S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de la liste.

8. Cochez la case J'accepte, puis choisissez Mettre à jour la liste.

API/CLI

Pour commencer les procédures suivantes, vous avez besoin de l'ID, tel que `trustedEntitySetId`, `threatEntitySetId`, ou `trustedIpSet`/`threatIpSet`, qui est associé à la ressource de liste que vous souhaitez mettre à jour.

Pour mettre à jour et activer une liste d'entités de confiance

1. Exécutez [UpdateTrustedEntitySet](#). Assurez-vous `detectorId` de fournir le compte membre pour lequel vous souhaitez mettre à jour cette liste d'entités de confiance. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.

Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante qui met à jour name la liste et active également cette liste :

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

`detector-id` Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez créer la liste des entités de confiance, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Que vous spécifiez ou non la valeur de ce paramètre, cela GuardDuty confirme que l' Compte AWS ID associé à cette `--detector-id` valeur possède le compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

S'applique uniquement aux menaces personnalisées et aux ensembles d'entités fiables personnalisés. Si vous fournissez une URL de localisation qui ne correspond pas aux formats pris en charge suivants, vous recevrez un message d'erreur lors de l'ajout et de l'activation de la liste.

Pour mettre à jour et activer une liste d'entités menaçantes

1. Exécutez [UpdateThreatEntitySet](#). Assurez-vous `detectorId` de fournir le compte membre pour lequel vous souhaitez créer cette liste d'entités menaçantes. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante qui met à jour name la liste et active également cette liste :

```
aws guardduty update-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--threat-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

`detector-id` Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez créer la liste des entités menaçantes, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Que vous spécifiez ou non la valeur de ce paramètre, cela GuardDuty confirme que l' ID Compte AWS associé à cette `--detector-id` valeur possède le compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

S'applique uniquement aux menaces personnalisées et aux ensembles d'entités fiables personnalisés. Si vous fournissez une URL de localisation qui ne correspond pas aux formats pris en charge suivants, vous recevrez un message d'erreur lors de l'ajout et de l'activation de la liste.

Pour mettre à jour et activer une liste d'adresses IP fiables

1. Exécutez [CreateIPSet](#). Assurez-vous `detectorId` de fournir le compte membre pour lequel vous souhaitez mettre à jour cette liste d'adresses IP fiables. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

Pour une liste d'adresses IP, le nom de votre liste doit être unique au sein d'une région Compte AWS et.

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante qui active également la liste :

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

`detector-id` Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez mettre à jour la liste d'adresses IP fiables, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Lorsque vous ne spécifiez pas l'ID de compte propriétaire du compartiment S3, aucune validation GuardDuty n'est effectuée. Lorsque vous spécifiez l'ID de compte pour le `expected-bucket-owner` paramètre, cela GuardDuty confirme que cet Compte AWS ID possède le compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

Pour ajouter et activer des listes d'adresses IP de menaces

1. Exécutez [CreateThreatIntelSet](#). Assurez-vous `detectorId` de fournir le compte membre pour lequel vous souhaitez créer cette liste d'adresses IP de menaces. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).

Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, un tiret (-) et un trait de soulignement (_).

Pour une liste d'adresses IP, le nom de votre liste doit être unique au sein d'une région Compte AWS et.

2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante qui active également la liste :

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

`detector-id` Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez mettre à jour la liste des adresses IP des menaces, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Si vous ne souhaitez pas activer cette liste nouvellement créée, remplacez le paramètre `--activate` par `--no-activate`.

Le paramètre `expected-bucket-owner` est facultatif. Lorsque vous ne spécifiez pas l'ID de compte propriétaire du compartiment S3, aucune validation GuardDuty n'est effectuée. Lorsque vous spécifiez l'ID de compte pour le `expected-bucket-owner` paramètre, cela GuardDuty confirme que cet Compte AWS ID possède le compartiment S3 spécifié dans le `--location` paramètre. S' GuardDuty il s'avère que ce compartiment S3 n'appartient pas à l'ID de compte spécifié, un message d'erreur s'affichera au moment de l'activation de cette liste.

De-activating liste d'entités ou liste d'adresses IP

Lorsque vous ne souhaitez plus GuardDuty utiliser une liste, vous pouvez la désactiver. La fin du processus peut prendre quelques minutes. Pour de plus amples informations, veuillez consulter [Considérations importantes relatives aux GuardDuty listes](#). Une fois la liste désactivée, les entrées de la liste d'entités ou de la liste d'adresses IP n'auront aucun impact sur la détection des menaces dans GuardDuty.

Choisissez l'une des méthodes d'accès pour désactiver la liste.

Console

Pour désactiver la liste d'entités ou la liste d'adresses IP

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Liste, sélectionnez l'onglet dans lequel vous souhaitez désactiver la liste : listes d'entités ou liste d'adresses IP.
4. Dans l'onglet sélectionné, sélectionnez la liste que vous souhaitez désactiver.
5. Choisissez Actions, puis sélectionnez Désactiver.
6. Confirmez l'action et choisissez Désactiver.

API/CLI

Pour commencer les procédures suivantes, vous avez besoin de l'ID, tel que `trustedEntitySetId` `threatEntitySetId` `trustedIpSet`, `outthreatIpSet`, associé à la ressource de liste que vous souhaitez désactiver.

Pour désactiver une liste d'entités de confiance

1. Exécutez [UpdateTrustedEntitySet](#). Assurez-vous `detectorId` de fournir le compte membre pour lequel vous souhaitez désactiver cette liste d'entités de confiance. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante :

```
aws guardduty update-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

`detector-id` Remplacez-le par l'ID du détecteur du compte membre pour lequel vous désactiverez la liste des entités de confiance, ainsi que par d'autres valeurs d'espace réservé qui le sont. *shown in red*

Pour désactiver les listes d'entités menaçantes

1. Exécutez [UpdateThreatEntitySet](#). Assurez-vous `detectorId` de fournir le compte membre pour lequel vous souhaitez désactiver cette liste d'entités menaçantes. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante :

```
aws guardduty update-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example \  

```

```
--no-activate
```

detector-id Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez créer la liste des entités menaçantes, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Pour désactiver une liste d'adresses IP fiables

1. Exécutez [UpdateIPSet](#). Assurez-vous de fournir le compte membre pour lequel vous souhaitez désactiver cette liste d'adresses IP fiables. detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante et en vous assurant de remplacer le par l'ID de détecteur du compte membre pour lequel vous désactiverez la liste d'adresses IP fiables.

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Pour désactiver la liste d'adresses IP des menaces

1. Exécutez [UpdateThreatIntelSet](#). Assurez-vous de fournir la liste detectorId d'adresses IP du compte membre pour lequel vous souhaitez désactiver cette liste d'adresses IP de menaces. detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectorsAPI](#).
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante et en vous assurant de remplacer le par l'ID du détecteur du compte membre pour lequel vous désactiverez la liste d'adresses IP des menaces.

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

```
--no-activate
```

Supprimer une liste d'entités ou une liste d'adresses IP

Lorsque vous ne souhaitez plus conserver une entrée de liste dans votre ensemble d'entités ou d'adresses IP, vous pouvez la supprimer. La fin du processus peut prendre quelques minutes. Pour de plus amples informations, veuillez consulter [Considérations importantes relatives aux GuardDuty listes](#).

Si le statut de la liste est Activation ou Désactivation, vous devez attendre quelques minutes avant d'effectuer une action. Pour de plus amples informations, veuillez consulter [Comprendre les statuts des listes](#).

Choisissez l'une des méthodes d'accès pour supprimer la liste.

Console

Pour supprimer une liste d'entités ou une liste d'adresses IP

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Liste, sélectionnez l'onglet dans lequel vous souhaitez supprimer la liste : listes d'entités ou liste d'adresses IP.
4. Dans l'onglet sélectionné, sélectionnez la liste que vous souhaitez supprimer.
5. Choisissez Actions, puis Supprimer.

Le statut de la liste deviendra Supprimer en attente. La suppression de la liste peut prendre quelques minutes.

API/CLI

Pour commencer les procédures suivantes, vous avez besoin de l'ID, tel que `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet`, `outhreatIpSet`, qui est associé à la ressource de liste que vous souhaitez supprimer.

Pour supprimer une liste d'entités de confiance

1. Exécutez [DeleteTrustedEntitySet](#). Assurez-vous de fournir le compte membre pour lequel vous souhaitez supprimer cette liste d'entités de confiance. Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante :

```
aws guardduty delete-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example
```

detector-id Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez supprimer la liste des entités de confiance, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Pour désactiver les listes d'entités menaçantes

1. Exécutez [DeleteThreatEntitySet](#). Assurez-vous de fournir le compte membre pour lequel vous souhaitez supprimer cette liste d'entités menaçantes. Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante :

```
aws guardduty delete-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

detector-id Remplacez-le par l'ID du détecteur du compte membre pour lequel vous allez supprimer la liste des entités menaçantes, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Pour supprimer une liste d'adresses IP fiables

1. Exécutez [DeleteIPSet](#). Assurez-vous de fournir le compte membre pour lequel vous souhaitez supprimer cette liste d'adresses IP de confiance. Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante et en vous assurant de remplacer le `detector-id` par l'ID de détecteur du compte membre pour lequel vous allez supprimer la liste d'adresses IP fiables.

```
aws guardduty delete-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example
```

Remplacez le `detector-id` par l'ID du détecteur du compte membre pour lequel vous allez supprimer la liste des entités menaçantes, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Pour supprimer la liste des adresses IP des menaces

1. Exécutez [DeleteThreatIntelSet](#). Assurez-vous de fournir le compte membre pour lequel vous souhaitez supprimer cette liste d'adresses IP de menaces. Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/console> ou exécutez l'[ListDetectors](#) API.
2. Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante et en vous assurant de remplacer le `detector-id` par l'ID du détecteur du compte membre pour lequel vous allez supprimer la liste des adresses IP des menaces.

```
aws guardduty delete-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example
```

Remplacez le `detector-id` par l'ID du détecteur du compte membre pour lequel vous allez supprimer la liste des entités menaçantes, ainsi que par d'autres valeurs d'espace réservé qui le sont *shown in red*.

Exportation des GuardDuty résultats générés vers des compartiments Amazon S3

GuardDuty conserve les résultats générés pendant une période de 90 jours. GuardDuty exporte les résultats actifs vers Amazon EventBridge (EventBridge). Vous pouvez éventuellement exporter les résultats générés vers un compartiment Amazon Simple Storage Service (Amazon S3). Cela vous aidera à suivre l'historique des activités potentiellement suspectes sur votre compte et à évaluer si les mesures correctives recommandées ont été couronnées de succès.

Tous les nouveaux résultats actifs GuardDuty générés sont automatiquement exportés dans les 5 minutes environ suivant leur génération. Vous pouvez définir la fréquence à laquelle les mises à jour des résultats actifs sont exportées EventBridge. La fréquence que vous sélectionnez s'applique à l'exportation de nouvelles occurrences de résultats existants vers EventBridge votre compartiment S3 (lorsqu'il est configuré) et Detective (lorsqu'il est intégré). Pour plus d'informations sur la manière dont les occurrences multiples de résultats existants sont GuardDuty agrégées, consultez [GuardDuty recherche d'agrégation](#).

Lorsque vous configurez les paramètres pour exporter les résultats vers un compartiment Amazon S3, GuardDuty utilise AWS Key Management Service (AWS KMS) pour chiffrer les données des résultats dans votre compartiment S3. Cela nécessite que vous ajoutiez des autorisations à votre compartiment S3 et à la AWS KMS clé afin que GuardDuty vous puissiez les utiliser pour exporter les résultats de votre compte.

Table des matières

- [Considérations](#)
- [Étape 1 — Autorisations requises pour exporter les résultats](#)
- [Étape 2 — Associer une politique à votre clé KMS](#)
- [Étape 3 — Associer une politique au compartiment Amazon S3](#)
- [Étape 4 - Exportation des résultats vers un compartiment S3 \(console\)](#)
- [Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour](#)

Considérations

Avant de passer aux conditions préalables et aux étapes à suivre pour exporter les résultats, considérez les concepts clés suivants :

- Les paramètres d'exportation sont régionaux : vous devez configurer les options d'exportation dans chaque région que vous utilisez GuardDuty.
- Exportation des résultats vers des compartiments Amazon S3 situés dans différents compartiments Régions AWS (entre régions) : GuardDuty prend en charge les paramètres d'exportation suivants :
 - Votre compartiment ou objet Amazon S3 et votre AWS KMS clé doivent appartenir au même compartiment Région AWS.
 - Pour les résultats générés dans une région commerciale, vous pouvez choisir d'exporter ces résultats vers un compartiment S3 dans n'importe quelle région commerciale. Cependant, vous ne pouvez pas exporter ces résultats vers un compartiment S3 situé dans une région optionnelle.
 - Pour les résultats générés dans une région optionnelle, vous pouvez choisir d'exporter ces résultats vers la même région optionnelle que celle dans laquelle ils ont été générés ou vers n'importe quelle région commerciale. Cependant, vous ne pouvez pas exporter les résultats d'une région optionnelle vers une autre région optionnelle.
- Autorisations d'exportation des résultats : pour configurer les paramètres d'exportation des résultats actifs, votre compartiment S3 doit disposer d'autorisations GuardDuty permettant de télécharger des objets. Vous devez également disposer d'une AWS KMS clé GuardDuty permettant de chiffrer les résultats.
- Les résultats archivés ne sont pas exportés — Le comportement par défaut est que les résultats archivés, y compris les nouvelles instances de résultats supprimés, ne sont pas exportés.

Lorsqu'une GuardDuty découverte est générée comme archivée, vous devez la désarchiver. Cela fait passer l'état de recherche du filtre à Actif. GuardDuty exporte les mises à jour des résultats non archivés existants en fonction de la façon dont vous les configurez [Étape 5 — Fréquence d'exportation des résultats](#).

- GuardDuty un compte administrateur peut exporter les résultats générés dans les comptes membres associés — Lorsque vous configurez les résultats d'exportation dans un compte administrateur, tous les résultats des comptes membres associés qui sont générés dans la même région sont également exportés vers le même emplacement que celui que vous avez configuré pour le compte administrateur. Pour de plus amples informations, veuillez consulter [Comprendre la relation entre le compte GuardDuty administrateur et les comptes membres](#).

Étape 1 — Autorisations requises pour exporter les résultats

Lorsque vous configurez les paramètres d'exportation des résultats, vous sélectionnez un compartiment Amazon S3 dans lequel vous pouvez stocker les résultats et une AWS KMS clé à

utiliser pour le chiffrement des données. Outre les autorisations relatives aux GuardDuty actions, vous devez également disposer des autorisations nécessaires pour effectuer les actions suivantes afin de configurer correctement les paramètres d'exportation des résultats :

- `s3:GetBucketLocation`
- `s3:PutObject`

Si vous devez exporter les résultats vers un préfixe spécifique de votre compartiment Amazon S3, vous devez également ajouter les autorisations suivantes au rôle IAM :

- `s3:GetObject`
- `s3:ListBucket`

Étape 2 — Associer une politique à votre clé KMS

GuardDuty chiffre les données de résultats de votre compartiment à l'aide AWS Key Management Service de. Pour configurer correctement les paramètres, vous devez d'abord GuardDuty autoriser l'utilisation d'une clé KMS. Vous pouvez accorder les autorisations en [attachant la stratégie](#) à votre clé KMS.

Lorsque vous utilisez une clé KMS provenant d'un autre compte, vous devez appliquer la politique de clé en vous connectant au Compte AWS propriétaire de la clé. Lorsque vous configurez les paramètres d'exportation des résultats, vous aurez également besoin de l'ARN clé du compte propriétaire de la clé.

Pour modifier la politique de clé KMS GuardDuty afin de chiffrer vos résultats exportés

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. Sélectionnez une clé KMS existante ou suivez les étapes pour [créer une nouvelle clé](#) dans le Guide du AWS Key Management Service développeur, que vous utiliserez pour crypter les résultats exportés.

 Note

La Région AWS valeur de votre clé KMS et celle du compartiment Amazon S3 doivent être identiques.

Vous pouvez utiliser le même compartiment S3 et la même paire de clés KMS pour exporter les résultats depuis n'importe quelle région applicable. Pour plus d'informations, consultez la section consacrée [Considérations](#) à l'exportation des résultats d'une région à l'autre.

4. Dans la section Key policy (Politique de clé), choisissez Edit (Modifier).

Si l'option Passer en mode stratégie s'affiche, choisissez-la pour afficher la politique clé, puis choisissez Modifier.

5. Copiez le bloc de politique suivant dans votre politique de clé KMS, pour GuardDuty autoriser l'utilisation de votre clé.

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

6. Modifiez la politique en remplaçant les valeurs suivantes qui sont mises en forme *red* dans l'exemple de stratégie :

1. *KMS key ARN* Remplacez-le par l'Amazon Resource Name (ARN) de la clé KMS. Pour localiser l'ARN de la clé, consultez la section [Recherche de l'ID de clé et de l'ARN](#) dans le Guide du AWS Key Management Service développeur.

2. **123456789012** Remplacez-le par l' Compte AWS identifiant propriétaire du GuardDuty compte exportant les résultats.
3. Remplacez **Region2** par l' Région AWS endroit où les GuardDuty résultats sont générés.
4. Remplacer **SourceDetectorID** par le detectorID nom du GuardDuty compte dans la région spécifique où les résultats ont été générés.

detectorId Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

 Note

Si vous utilisez GuardDuty dans une région optionnelle, remplacez la valeur du « Service » par le point de terminaison régional de cette région. Par exemple, si vous utilisez GuardDuty dans la région Moyen-Orient (Bahreïn) (me-south-1), remplacez par "Service": "guardduty.amazonaws.com". "Service": "guardduty.me-south-1.amazonaws.com" Pour plus d'informations sur les points de terminaison pour chaque région optionnelle, consultez la section [GuardDuty Points de terminaison et quotas](#).

7. Si vous avez ajouté la déclaration de politique avant la déclaration finale, ajoutez une virgule avant d'ajouter cette déclaration. Assurez-vous que la syntaxe JSON de votre politique de clé KMS est valide.

Choisissez Enregistrer.

8. (Facultatif) copiez l'ARN de la clé dans un bloc-notes pour l'utiliser ultérieurement.

Étape 3 — Associer une politique au compartiment Amazon S3

Ajoutez des autorisations au compartiment Amazon S3 vers lequel vous allez exporter les résultats afin que vous GuardDuty puissiez télécharger des objets dans ce compartiment S3. Indépendamment de l'utilisation d'un compartiment Amazon S3 appartenant à votre compte ou à un autre Compte AWS, vous devez ajouter ces autorisations.

Si, à tout moment, vous décidez d'exporter les résultats vers un autre compartiment S3, pour continuer à exporter les résultats, vous devez ajouter des autorisations à ce compartiment S3 et configurer à nouveau les paramètres d'exportation des résultats.

Si vous ne possédez pas encore de compartiment Amazon S3 dans lequel vous souhaitez exporter ces résultats, consultez la section [Création d'un compartiment](#) dans le guide de l'utilisateur Amazon S3.

Pour associer des autorisations à votre politique de compartiment S3

1. Suivez les étapes décrites dans la section [Pour créer ou modifier une politique de compartiment](#) dans le guide de l'utilisateur Amazon S3, jusqu'à ce que la page Modifier la politique de compartiment apparaisse.
2. L'exemple de politique montre comment accorder GuardDuty l'autorisation d'exporter les résultats vers votre compartiment Amazon S3. Si vous modifiez le chemin après avoir configuré les résultats de l'exportation, vous devez modifier la politique pour accorder l'autorisation d'accéder au nouvel emplacement.

Copiez l'exemple de politique suivant et collez-le dans l'éditeur de politiques Bucket.

Si vous avez ajouté la déclaration de politique avant la déclaration finale, ajoutez une virgule avant d'ajouter cette déclaration. Assurez-vous que la syntaxe JSON de votre politique de clé KMS est valide.

Exemple de stratégie de compartiment S3

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow GetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
```

```

        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"
        }
    },
    {
        "Sid": "Allow PutObject",
        "Effect": "Allow",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012",
                "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"
            }
        }
    },
    {
        "Sid": "Deny unencrypted object uploads",
        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "aws:kms"
            }
        }
    },
    {
        "Sid": "Deny incorrect encryption header",
        "Effect": "Deny",

```

```

        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
    **",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
                "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        }
    },
    {
        "Sid": "Deny non-HTTPS access",
        "Effect": "Deny",
        "Principal": "**",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
    **",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        }
    }
]
}

```

3. Modifiez la politique en remplaçant les valeurs suivantes qui sont mises en forme *red* dans l'exemple de stratégie :
 1. *Amazon S3 bucket ARN* Remplacez-le par le nom de ressource Amazon (ARN) du compartiment Amazon S3. L'ARN du bucket se trouve sur la page Modifier la politique du bucket de la <https://console.aws.amazon.com/s3/> console.
 2. *123456789012* Remplacez-le par l' Compte AWS identifiant propriétaire du GuardDuty compte exportant les résultats.
 3. Remplacez *us-east-2* par l' Région AWS endroit où les GuardDuty résultats sont générés.
 4. Remplacer *SourceDetectorID* par le detectorID nom du GuardDuty compte dans la région spécifique où les résultats ont été générés.

detectorIdPour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la <https://console.aws.amazon.com/guardduty/> console ou exécutez l'[ListDetectorsAPI](#).

5. Remplacez une *[optional prefix]* partie de la valeur de l'*S3 bucket ARN/[optional prefix]* espace réservé par un emplacement de dossier facultatif vers lequel vous souhaitez exporter les résultats. Pour plus d'informations sur l'utilisation des préfixes, consultez la section [Organisation des objets à l'aide de préfixes](#) dans le guide de l'utilisateur Amazon S3.

Lorsque vous indiquez un emplacement de dossier facultatif, le dossier doit déjà exister dans le compartiment S3. GuardDuty ne crée pas le dossier en votre nom. Cette exigence s'applique quel que soit le propriétaire du compartiment.

6. Remplacez *KMS key ARN* par l'Amazon Resource Name (ARN) de la clé KMS associée au chiffrement des résultats exportés vers le compartiment S3. Pour localiser l'ARN de la clé, consultez la section [Recherche de l'ID de clé et de l'ARN](#) dans le Guide du AWS Key Management Service développeur.

Note

Si vous utilisez GuardDuty dans une région optionnelle, remplacez la valeur du « Service » par le point de terminaison régional de cette région. Par exemple, si vous utilisez GuardDuty dans la région Moyen-Orient (Bahreïn) (me-south-1), remplacez par "Service": "guardduty.amazonaws.com". "Service": "guardduty.me-south-1.amazonaws.com" Pour plus d'informations sur les points de terminaison pour chaque région optionnelle, consultez la section [GuardDuty Points de terminaison et quotas](#).

4. Choisissez Enregistrer.

Étape 4 - Exportation des résultats vers un compartiment S3 (console)

GuardDuty vous permet d'exporter les résultats vers un compartiment existant dans un autre Compte AWS.

Lorsque vous créez un nouveau compartiment S3 ou que vous choisissez un compartiment existant dans votre compte, vous pouvez ajouter un préfixe facultatif. Le préfixe et le chemin du dossier dans lesquels les résultats sont écrits doivent déjà exister dans le compartiment S3. GuardDuty

ne crée aucun dossier en votre nom. GuardDuty écrit les objets des résultats dans le chemin/
AWSLogs/**123456789012**/GuardDuty/**Region**. Vous devez donc créer cette structure de dossiers
avant d'exporter les résultats.

Le chemin complet de l'objet S3 sera **amzn-s3-demo-bucket/prefix-name/UUID.jsonl.gz**.
Le UUID est généré de manière aléatoire et ne représente pas l'identifiant du détecteur ou l'identifiant
de la découverte.

 Important

La clé KMS doit se trouver dans la même région que le compartiment S3.

Avant de terminer ces étapes, assurez-vous d'avoir joint les politiques correspondantes à votre clé
KMS et à votre compartiment S3 existant.

Pour configurer les résultats de l'exportation

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, sous Options d'exportation des résultats, pour le compartiment S3, choisissez Configurer maintenant (ou Modifier, selon les besoins).
4. Pour l'ARN du compartiment S3, entrez le **bucket ARN**. Pour trouver l'ARN du compartiment, consultez la section [Affichage des propriétés d'un compartiment S3](#) dans le guide de l'utilisateur Amazon S3.
5. Pour l'ARN de la clé KMS, entrez le **key ARN**. Pour localiser l'ARN de la clé, consultez la section [Recherche de l'ID de clé et de l'ARN](#) dans le Guide du AWS Key Management Service développeur.
6. Joindre des politiques
 - Suivez les étapes pour joindre la politique de compartiment S3. Pour de plus amples informations, veuillez consulter [Étape 3 — Associer une politique au compartiment Amazon S3](#).
 - Suivez les étapes pour joindre la politique de clé KMS. Pour de plus amples informations, veuillez consulter [Étape 2 — Associer une politique à votre clé KMS](#).
7. Choisissez Enregistrer.

Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour

Configurez la fréquence d'exportation des résultats actifs mis à jour en fonction de votre environnement. Par défaut, les conclusions mises à jour sont exportées toutes les 6 heures. Cela signifie que tous les résultats mis à jour après l'exportation la plus récente sont inclus dans la nouvelle exportation. Si les résultats mis à jour sont exportés toutes les 6 heures et que l'exportation se produit à 12 h, tout résultat mis à jour après 12 h est exporté à 18 h.

Pour définir la fréquence

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Cliquez sur Paramètres.
3. Dans la section Options d'exportation des résultats choisissez Fréquence des résultats mis à jour. Cela définit la fréquence d'exportation des résultats Active mis à jour à la fois vers Amazon S3 EventBridge et vers Amazon S3. Sélectionnez parmi les éléments suivants :
 - Mise à jour EventBridge et S3 toutes les 15 minutes
 - Mise à jour EventBridge et S3 toutes les 1 heure
 - Mise à jour EventBridge et S3 toutes les 6 heures (par défaut)
4. Sélectionnez Enregistrer les modifications.

Traitement des GuardDuty résultats avec Amazon EventBridge

GuardDuty publie (envoie) automatiquement les résultats sous forme d'événements à Amazon EventBridge (anciennement Amazon CloudWatch Events), un service de bus d'événements sans serveur. EventBridge fournit un flux de données en temps quasi réel provenant d'applications et de services à des cibles telles que les rubriques AWS Lambda, les fonctions Amazon Simple Notification Service (Amazon SNS) et les flux Amazon Kinesis. Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

EventBridge permet le suivi et le traitement automatisés des GuardDuty résultats en recevant [des événements](#). EventBridge reçoit des événements à la fois pour les résultats nouvellement générés et pour les résultats agrégés, lorsque les occurrences ultérieures d'un résultat existant sont combinées avec l'original. Chaque GuardDuty découverte se voit attribuer un identifiant de recherche et GuardDuty crée un EventBridge événement pour chaque découverte avec un identifiant

de recherche unique. Pour plus d'informations sur le fonctionnement de l'agrégation GuardDuty, voir [GuardDuty recherche d'agrégation](#).

Outre la surveillance et le traitement automatisés, l'utilisation de EventBridge permet de conserver à long terme les données de vos résultats. GuardDuty conserve les résultats pendant 90 jours. Vous pouvez ainsi envoyer les données des résultats vers votre plateforme de stockage préférée et les stocker aussi longtemps que vous le souhaitez. EventBridge Pour conserver les résultats plus longtemps, GuardDuty les supports [Exportation des résultats générés vers Amazon S3](#).

Rubriques

- [Comprendre la fréquence des EventBridge notifications dans GuardDuty](#)
- [Configurer une rubrique et un point de terminaison Amazon SNS \(e-mail, Slack et Amazon Chime\)](#)
- [Utiliser Amazon EventBridge pour les GuardDuty résultats](#)
- [Création d'une EventBridge règle pour les GuardDuty résultats](#)
- [EventBridge règle pour les GuardDuty environnements multi-comptes](#)

Comprendre la fréquence des EventBridge notifications dans GuardDuty

Cette section explique à quelle fréquence vous recevez des notifications de recherche EventBridge et comment mettre à jour la fréquence pour les occurrences de recherche ultérieures.

Notifications pour les résultats nouvellement générés avec un identifiant de recherche unique

GuardDuty envoie ces notifications en temps quasi réel lorsqu'il génère un résultat avec un identifiant de recherche unique. La notification inclut toutes les occurrences ultérieures de cet identifiant de recherche au cours du processus de génération de notification.

La fréquence des notifications pour les nouvelles découvertes se fait en temps quasi réel. Par défaut, vous ne pouvez pas modifier cette fréquence.

Notifications pour les occurrences de résultat ultérieures

GuardDuty regroupe en un seul événement toutes les occurrences ultérieures d'un type de découverte particulier qui se produisent dans les intervalles de 6 heures. Seul un compte administrateur peut mettre à jour la fréquence des EventBridge notifications pour les occurrences de détection ultérieures. Un compte membre ne peut pas mettre à jour cette fréquence pour son propre compte. Par exemple, si le compte d' GuardDuty administrateur délégué met à jour la

fréquence à une heure, tous les comptes membres seront également soumis à une fréquence de notification d'une heure concernant les occurrences de recherche ultérieures envoyées à EventBridge. Pour plus d'informations, consultez [Gérer plusieurs comptes sur Amazon GuardDuty](#).

En tant que compte administrateur, vous pouvez personnaliser la fréquence par défaut des notifications concernant les occurrences de recherche ultérieures. Les valeurs possibles sont 15 minutes, 1 heure ou, par défaut, 6 heures. Pour plus d'informations sur la configuration de la fréquence de ces notifications, veuillez consulter [Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour](#).

Pour plus de détails sur la réception de EventBridge notifications par le compte administrateur pour les comptes membres, consultez [EventBridge règle pour les environnements multi-comptes](#).

Configurer une rubrique et un point de terminaison Amazon SNS (e-mail, Slack et Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) est un service entièrement géré qui permet aux éditeurs de transmettre des messages aux abonnés. Les éditeurs communiquent de manière asynchrone avec les abonnés en envoyant des messages à un sujet. Une rubrique est un point d'accès logique et un canal de communication qui vous permettent de regrouper plusieurs points de terminaison tels qu' AWS Lambda Amazon Simple Queue Service (Amazon SQS) et une adresse e-mail HTTP/S.

Note

Vous pouvez ajouter une rubrique Amazon SNS à votre règle d' EventBridge événement préférée pendant ou après la création de la règle.

Création d'une rubrique Amazon SNS

Pour commencer, vous devez d'abord configurer une rubrique dans Amazon SNS et ajouter un point de terminaison. Pour créer un sujet, suivez les étapes décrites à l'[étape 1 : Création d'un sujet](#) dans le manuel Amazon Simple Notification Service Developer Guide. Une fois le sujet créé, copiez l'ARN du sujet dans le presse-papiers. Vous allez utiliser l'ARN de cette rubrique pour continuer avec l'une des configurations préférées.

Choisissez une méthode préférée pour déterminer où vous souhaitez envoyer les données de GuardDuty recherche.

Email setup

Pour configurer un point de terminaison de messagerie

Ensuite [Create an Amazon SNS topic](#), l'étape suivante consiste à créer un abonnement à cette rubrique. Suivez les étapes décrites à l'[étape 2 : Création d'un abonnement à une rubrique Amazon SNS](#) dans le guide du développeur Amazon Simple Notification Service.

1. Pour l'ARN du sujet, utilisez l'ARN du sujet créé à l'[Create an Amazon SNS topic](#) étape. L'ARN de la rubrique ressemble à ce qui suit :

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. Pour Protocol, sélectionnez Email.
3. Pour Endpoint, entrez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications d'Amazon SNS.

Une fois l'abonnement créé, vous devrez le confirmer par le biais de votre client de messagerie.

Slack setup

Pour configurer un développeur Amazon Q dans un client d'applications de chat - Slack

Ensuite [Create an Amazon SNS topic](#), l'étape suivante consiste à configurer le client pour Slack.

Suivez les étapes décrites dans la section [Tutoriel : Commencez à utiliser Slack](#) dans le guide de l'administrateur des applications de chat Amazon Q destiné aux développeurs.

Chime setup

Pour configurer un développeur Amazon Q dans un client d'applications de chat - Chime

Ensuite [Create an Amazon SNS topic](#), l'étape suivante consiste à configurer Amazon Q Developer pour Chime.

Suivez les étapes décrites dans [Tutoriel : Démarrez avec Amazon Chime](#) dans le Guide de l'administrateur des applications de chat Amazon Q destinées aux développeurs.

Utiliser Amazon EventBridge pour les GuardDuty résultats

Avec EventBridge, vous créez des règles pour spécifier les événements que vous souhaitez surveiller. Ces règles spécifient également les services et applications cibles qui peuvent effectuer des actions automatisées si ces événements se produisent. Une [cible](#) est une destination (une ressource ou un point de terminaison) qui EventBridge envoie un événement lorsque celui-ci correspond au modèle d'événement défini dans la règle. Chaque événement est un objet JSON conforme au EventBridge schéma des AWS événements et contenant une représentation JSON d'un résultat. Vous pouvez adapter la règle pour n'envoyer que les événements répondant à certains critères. Pour plus d'informations, consultez [the section called "Schéma d'événement"](#). Les données des résultats étant structurées sous la forme d'un [EventBridgeévénement](#), vous pouvez surveiller, traiter et agir en fonction des résultats en utilisant d'autres applications, services et outils.

Pour recevoir des notifications concernant les GuardDuty résultats basés sur des événements, vous devez créer une EventBridge règle et un objectif pour GuardDuty. Cette règle permet EventBridge d'envoyer des notifications pour les résultats GuardDuty générés à la cible spécifiée dans la règle.

Note

EventBridge et les CloudWatch événements sont le même service sous-jacent et la même API. Cependant, il EventBridge inclut des fonctionnalités supplémentaires qui vous aident à recevoir des événements provenant d'applications SaaS (Software as a Service) et de vos propres applications. Le service sous-jacent et l'API étant identiques, le schéma des événements pour les GuardDuty résultats est également le même.

Comment GuardDuty fonctionnent les résultats archivés et non archivés EventBridge

Pour les résultats que vous archivez manuellement, les occurrences initiales et suivantes de ces résultats (générées une fois l'archivage terminé) sont envoyées en EventBridge fonction d'une fréquence de notification spécifique. Pour plus d'informations, consultez [Comprendre la fréquence des EventBridge notifications dans GuardDuty](#).

Pour les résultats qui sont automatiquement archivés avec [Règles de suppression](#), les occurrences initiales et suivantes de ces résultats (générées une fois l'archivage terminé) ne sont pas envoyées à EventBridge. Vous pouvez consulter ces résultats archivés automatiquement dans la GuardDuty console.

Schéma d'événement

Un [modèle d'événement](#) définit les données EventBridge utilisées pour déterminer s'il faut envoyer l'événement à la cible. L' EventBridge événement pour GuardDuty a le format suivant :

```
{
  "version": "0",
  "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
  "detail-type": "GuardDuty Finding",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "1970-01-01T00:00:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

La `detail` valeur renvoie les détails JSON d'une seule constatation sous forme d'objet, au lieu de renvoyer l'intégralité de la syntaxe de réponse aux résultats, qui prend en charge plusieurs résultats dans un tableau.

Pour une liste complète de tous les paramètres inclus `GUARDDUTY_FINDING_JSON_OBJECT`, voir [GetFindings](#). Le paramètre `id` qui apparaît dans `GUARDDUTY_FINDING_JSON_OBJECT` est l'ID du résultat décrit précédemment.

Création d'une EventBridge règle pour les GuardDuty résultats

Les procédures suivantes expliquent comment utiliser la EventBridge console Amazon et le [AWS Command Line Interface \(AWS CLI\)](#) pour créer une EventBridge règle pour les GuardDuty résultats. La règle détecte les EventBridge événements qui utilisent le schéma et le modèle d'événements pour GuardDuty les résultats, et elle envoie ces événements à une AWS Lambda fonction pour traitement.

AWS Lambda est un service de calcul que vous pouvez utiliser pour exécuter du code sans provisionner ni gérer de serveurs. Vous empaqueter votre code et le télécharger en AWS Lambda tant que fonction Lambda. AWS Lambda exécute ensuite la fonction lorsque la fonction est invoquée. Une fonction peut être appelée manuellement, par vous, automatiquement en réponse à des événements, ou en réponse à des demandes d'applications ou de services. Pour en savoir plus sur la création et l'invocation de fonctions Lambda, consultez le [Guide du développeur AWS Lambda](#).

Choisissez votre méthode préférée pour créer une EventBridge règle qui envoie votre GuardDuty résultat à une cible.

Console

Suivez ces étapes pour utiliser la EventBridge console Amazon afin de créer une règle qui envoie automatiquement tous les événements de GuardDuty recherche à une fonction Lambda pour traitement. La règle utilise les paramètres par défaut pour les règles qui s'exécutent lorsque des événements spécifiques sont reçus. Pour en savoir plus sur les paramètres des règles ou pour savoir comment créer une règle utilisant des paramètres personnalisés, consultez la section [Création de règles qui réagissent aux événements](#) dans le guide de EventBridge l'utilisateur Amazon.

Avant de créer cette règle, créez la fonction Lambda que vous souhaitez que la règle utilise comme cible. Lorsque vous créez la règle, vous devez spécifier cette fonction comme étant la cible de la règle. Votre cible peut également être le sujet SNS que vous avez créé précédemment. Pour plus d'informations, consultez [Configurer une rubrique et un point de terminaison Amazon SNS \(e-mail, Slack et Amazon Chime\)](#).

Pour créer une règle d'événement à l'aide de la console

1. Connectez-vous à la EventBridge console Amazon Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/events/>.
2. Dans le volet de navigation, sous Bus, sélectionnez Rules.
3. Dans la section Rules (Règles) choisissez Create rule (Créer une règle).
4. Sur la page détaillée de définition de la règle, procédez comme suit :
 - a. Pour Name (Nom), entrez le nom de la règle.
 - b. (Facultatif) Dans Description, entrez une brève description de la règle.
 - c. Pour le bus d'événements, assurez-vous que la valeur par défaut est sélectionnée et que l'option Activer la règle sur le bus d'événements sélectionné est activée.
 - d. Pour Type de règle, choisissez Règle avec un modèle d'événement.
 - e. Lorsque vous avez terminé, choisissez Suivant.
5. Sur la page Créer un modèle d'événement, procédez comme suit :
 - a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
 - b. (Facultatif) Pour Exemple d'événement, consultez un exemple d'événement de recherche GuardDuty pour savoir ce qu'un événement peut contenir. Pour ce faire,

choisissez AWS des événements. Ensuite, dans la section Exemples d'événements, choisissez GuardDutyFinding.

- c. Option 1 - Utilisation du formulaire de modèle, un modèle qui EventBridge fournit

Dans la section Modèle d'événement, vous pouvez effectuer les opérations suivantes :

1. Pour Méthode de création, sélectionnez Utiliser le formulaire de modèle.
2. Pour Event source (Source d'événement), choisissez Services AWS.
3. Pour Service AWS, choisissez GuardDuty.
4. Pour Type d'événement, choisissez GuardDuty Finding (Résultat Amazon Macie).

Lorsque vous avez terminé, choisissez Suivant.

- d. Option 2 - Utilisation d'un modèle d'événement personnalisé dans JSON

Dans la section Modèle d'événement, vous pouvez effectuer les opérations suivantes :

1. Pour Méthode de création, sélectionnez Modèle personnalisé (éditeur JSON).
2. Pour le modèle d'événement, collez le code JSON personnalisé suivant qui créera une alerte pour les résultats moyens, élevés et critiques. Pour plus d'informations, consultez [Niveaux de gravité des résultats](#).

```
{
  "source": [
    "aws.guarddduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
```

4.8,
4.9,
5,
5.0,
5.1,
5.2,
5.3,
5.4,
5.5,
5.6,
5.7,
5.8,
5.9,
6,
6.0,
6.1,
6.2,
6.3,
6.4,
6.5,
6.6,
6.7,
6.8,
6.9,
7,
7.0,
7.1,
7.2,
7.3,
7.4,
7.5,
7.6,
7.7,
7.8,
7.9,
8,
8.0,
8.1,
8.2,
8.3,
8.4,
8.5,
8.6,
8.7,

```
    8.8,  
    8.9,  
    9,  
    9.0,  
    9.1,  
    9.2,  
    9.3,  
    9.4,  
    9.5,  
    9.6,  
    9.7,  
    9.8,  
    9.9,  
    10,  
    10.0  
  ]  
}  
}
```

Lorsque vous avez terminé, choisissez Suivant.

6. Option A - Sélection Service AWS - AWS Lambda comme cible

Sur la page Sélectionner une ou plusieurs cibles, procédez comme suit :

- a. Pour les types de cibles, sélectionnez Service AWS.
- b. Pour Select a target (Sélectionner une cible), choisissez Lambda Function (Fonction Lambda). Ensuite, pour Function, choisissez la fonction Lambda à laquelle vous souhaitez envoyer des événements de recherche.
- c. Pour Configurer version/alias, entrez les paramètres de version ou d'alias pour la fonction Lambda cible.
- d. (Facultatif) Pour Paramètres supplémentaires, entrez des paramètres personnalisés pour spécifier les données d'événement que vous souhaitez envoyer à la fonction Lambda. Vous pouvez également spécifier comment gérer les événements qui ne sont pas transmis correctement à la fonction.
- e. Lorsque vous avez terminé, choisissez Suivant.

7. Option B - Sélection du sujet SNS comme cible

Sur la page Sélectionner une ou plusieurs cibles, procédez comme suit :

- a. Pour les types de cibles, sélectionnez Service AWS.
- b. Pour Sélectionner une cible, choisissez Rubrique SNS. Ensuite, pour Emplacement cible, sélectionnez l'option appropriée en fonction de votre emplacement cible. Pour Rubrique, choisissez le nom de la rubrique SNS que vous avez créée.
- c. Développer Additional settings (Paramètres supplémentaires). Pour Configurer l'entrée cible, choisissez Transformateur d'entrée.
- d. Choisissez Configure input transformer (Configurer le transformateur d'entrée).
- e. Copiez le code suivant et collez-le dans le champ Chemin d'entrée sous la section Transformateur d'entrée cible.

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

- f. Copiez le code suivant et collez-le dans le champ Modèle pour formater l'e-mail.

```
{"message": "You have a severity <severity> GuardDuty finding type  
<Finding_Type> in the <region> Region.\n\nFinding Description:  
\n<Finding_Description>\n\nFor more details open the GuardDuty console at  
https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?  
search=id%3D<Finding_ID>"}}
```

 Important

Fournissez le modèle sous la forme d'un objet JSON sur une seule ligne, avec le message enveloppé dans une clé telle message que celle illustrée dans l'exemple précédent. \nÀ utiliser pour ajouter des sauts de ligne.

GuardDuty recherche de champs tels que ceux qui description peuvent contenir des caractères de contrôle non échappés, y compris des nouvelles lignes. N'utilisez aucun des formats de modèle suivants :

- Une chaîne entre guillemets
- Un modèle multiligne qui utilise des chaînes entre guillemets distinctes sur des lignes distinctes

Avec ces formats, la valeur substituée peut produire du JSON non valide. EventBridge rejette ensuite l'événement et ne transmet pas la notification.

 Note

Les abonnements par e-mail reçoivent le modèle de sortie tel quel, de sorte que l'e-mail affiche l'objet message JSON et les sauts de ligne apparaissent tels quels\n. Pour les notifications formatées, transmettez la rubrique Amazon SNS à Amazon Q Developer dans des applications de chat (Slack ou Amazon Chime), ou utilisez une fonction Lambda comme cible.

8. Sur la page Configurer les balises, entrez éventuellement une ou plusieurs balises à attribuer à la règle. Ensuite, sélectionnez Suivant.
9. Sur la page Réviser et créer, passez en revue les paramètres de la règle et vérifiez qu'ils sont corrects.

Pour modifier un paramètre, choisissez Modifier dans la section contenant le paramètre, puis entrez le paramètre correct. Vous pouvez également utiliser les onglets de navigation pour accéder à la page contenant un paramètre.

10. Lorsque vous avez terminé de vérifier les paramètres, choisissez Create rule.

API

La procédure suivante montre comment utiliser des AWS CLI commandes pour créer une EventBridge règle et une cible pour GuardDuty. Plus précisément, la procédure explique comment créer une règle qui permet d' EventBridge envoyer des événements pour tous les résultats GuardDuty générés à une AWS Lambda fonction en tant que cible pour la règle.

 Note

Dans cet exemple, nous utilisons une fonction Lambda comme cible pour la règle qui se déclenche. EventBridge Vous pouvez également configurer d'autres AWS ressources comme cibles à déclencher EventBridge. GuardDuty et EventBridge prennent en charge les types de cibles suivants : les instances Amazon EC2, les flux Amazon Kinesis, les tâches Amazon ECS, les machines d'état AWS Step Functions , run la commande et les cibles intégrées. Pour plus d'informations, consultez [PutTargets](#)le Amazon EventBridge API Reference.

Pour créer une règle et une cible

1. Pour créer une règle permettant d' EventBridge envoyer des événements pour tous les résultats GuardDuty générés, exécutez la commande EventBridge CLI suivante.

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guardduty\"]}"
```

Vous pouvez personnaliser davantage votre règle afin qu'elle indique d' EventBridge envoyer des événements uniquement pour un sous-ensemble des GuardDuty-generated résultats. Ce sous-ensemble est basé sur le ou les attributs de résultat qui sont spécifiés dans la règle. Par exemple, utilisez la commande CLI suivante pour créer une règle qui permet EventBridge d'envoyer des événements uniquement pour les GuardDuty résultats présentant une gravité de 5 ou 8 :

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":  
{\"severity\":[5,8]}}"
```

À cette fin, vous pouvez utiliser n'importe quelle valeur de propriété disponible dans le JSON pour les GuardDuty résultats.

2. Pour associer une fonction Lambda comme cible à la règle que vous avez créée à l'étape 1, exécutez la commande EventBridge CLI suivante.

```
aws events put-targets --rule your-rule-name --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your-function
```

Assurez-vous de `your-rule-name` remplacer par le nom de la règle que vous avez créée à l'étape 1 et `your-function` par votre fonction Lambda réelle pour les GuardDuty événements.

3. Pour ajouter les autorisations requises pour invoquer la cible, exécutez la commande d'interface de ligne de commande Lambda suivante.

```
aws lambda add-permission --function-name your-function --statement-id 1 --  
action 'lambda:InvokeFunction' --principal events.amazonaws.com --source-arn  
arn:aws:events:us-east-1:111122223333:rule/your-rule-name
```

Assurez-vous de `your-function` remplacer par votre fonction Lambda réelle pour les GuardDuty événements et par le nom `your-rule-name` de la règle que vous avez créée à l'étape 1. La `--source-arn` condition permet uniquement à cette règle d'invoquer la fonction.

EventBridge règle pour les GuardDuty environnements multi-comptes

Lorsque vous utilisez un compte d' GuardDuty administrateur délégué, vous pouvez consulter les événements générés dans les comptes des membres et prendre des mesures à l'aide d'autres applications et services. EventBridge les règles de votre compte administrateur seront déclenchées en fonction des résultats applicables de vos comptes de membre. Si vous configurez les notifications de recherche via EventBridge votre compte administrateur, vous recevrez des notifications de résultats à la fois de votre compte et des comptes des membres. Par exemple, vous pouvez l'utiliser EventBridge pour envoyer des types spécifiques de résultats à une fonction Lambda qui traite et envoie les données à votre système de gestion des incidents et des événements de sécurité (SIEM).

Vous pouvez identifier le compte membre d'où provient la GuardDuty recherche à l'aide du `accountId` champ contenant les détails JSON de la recherche. Pour créer une règle d'événement personnalisée pour des comptes de membres spécifiques, créez une nouvelle règle et utilisez le modèle suivant dans Modèle d'événement. Remplacez `123456789012` par `accountId` celui du compte membre pour lequel vous souhaitez déclencher l'événement.

```
{  
  "source": [  
    "aws.guardduty"  
  ],  
  "detail-type": [  

```

```
"GuardDuty Finding"
],
"detail": {
  "accountId": [
    "123456789012"
  ]
}
}
```

Note

Cet exemple crée une règle qui correspond à tous les résultats de l'ID de compte spécifié. Vous pouvez inclure plusieurs identifiants de compte en les séparant par des virgules, conformément à la syntaxe JSON.

Comprendre CloudWatch les journaux et les raisons pour lesquelles des ressources sont ignorées lors de l'analyse Malware Protection for EC2

GuardDuty Malware Protection for EC2 publie les événements dans votre groupe de CloudWatch journaux Amazon/aws/guardduty/malware-scan-events. Pour chacun des événements liés à l'analyse des programmes malveillants, vous pouvez surveiller l'état et le résultat de l'analyse de vos ressources concernées. Certaines ressources Amazon EC2 et certains volumes Amazon EBS ont peut-être été ignorés lors de l'analyse Malware Protection for EC2.

CloudWatch Journaux d'audit dans GuardDuty Malware Protection pour EC2

Trois types d'événements d'analyse sont pris en charge dans le groupe de journaux/aws/guardduty/malware-scan-events. CloudWatch

Nom de l'événement d'analyse Malware Protection for EC2	Explication
EC2_SCAN_STARTED	Créé lorsqu'une protection contre les GuardDuty programmes malveillants pour EC2

Nom de l'événement d'analyse Malware Protection for EC2	Explication
	lance le processus d'analyse des programmes malveillants, par exemple en préparant la prise d'un instantané d'un volume EBS.
EC2_SCAN_COMPLETED	Créé lorsque l'analyse de GuardDuty Malware Protection for EC2 est terminée pour au moins un des volumes EBS de la ressource concernée. Cet événement inclut également l' <code>snapshotId</code> qui appartient au volume EBS analysé. Une fois l'analyse terminée, son résultat de l'analyse sera <code>CLEAN</code> , <code>THREATS_FOUND</code> ou <code>NOT_SCANNED</code> .
EC2_SCAN_SKIPPED	Créé lorsque GuardDuty Malware Protection for EC2 scan ignore tous les volumes EBS de la ressource concernée. Pour identifier le motif de l'omission, sélectionnez l'événement correspondant et consultez les détails. Pour plus d'informations sur les motifs de l'omission, veuillez consulter Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants ci-dessous.

 Note

Si vous utilisez un AWS Organizations, les événements de CloudWatch journal des comptes membres dans Organisations sont publiés à la fois sur le compte administrateur et sur le groupe de journaux du compte membre.

Choisissez votre méthode d'accès préférée pour consulter et interroger CloudWatch les événements.

Console

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, choisissez Journaux, Groupes de journaux. Choisissez le groupe de journaux/aws/guardduty/malware-scan-events pour afficher les événements d'analyse pour Malware Protection for EC2. GuardDuty

Pour exécuter une requête, choisissez Log Insights.

Pour plus d'informations sur l'exécution d'une requête, consultez la section [Analyse des données de journal avec CloudWatch Logs Insights](#) dans le guide de CloudWatch l'utilisateur Amazon.

3. Choisissez Analyser l'ID pour surveiller les détails de la ressource concernée et les résultats de logiciels malveillants. Par exemple, vous pouvez exécuter la requête suivante pour filtrer les événements du CloudWatch journal à l'aide de scanId. Assurez-vous d'utiliser votre propre code valide *scan-id*.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- Pour travailler avec des groupes de journaux, consultez [la section Rechercher des entrées de journal AWS CLI](#) à l'aide du guide de CloudWatch l'utilisateur Amazon.

Choisissez le groupe de journaux/aws/guardduty/malware-scan-events pour afficher les événements d'analyse pour Malware Protection for EC2. GuardDuty

- Pour afficher et filtrer les événements du journal, consultez [GetLogEvents](#) et [FilterLogEvents](#), respectivement, dans le manuel Amazon CloudWatch API Reference.

GuardDuty Protection contre les programmes malveillants pour la conservation des journaux EC2

La période de conservation des journaux par défaut pour le groupe de journaux/aws/guardduty/malware-scan-events est de 90 jours, après quoi les événements du journal sont automatiquement

supprimés. Pour modifier la politique de conservation des journaux pour votre groupe de CloudWatch journaux, voir [Modifier la conservation des données des CloudWatch journaux dans Logs](#) dans le guide de CloudWatch l'utilisateur Amazon ou [PutRetentionPolicy](#) dans la référence de l' CloudWatch API Amazon.

Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants

Lors des événements liés à l'analyse des programmes malveillants, certaines ressources EC2 et certains volumes EBS peuvent avoir été ignorés pendant le processus d'analyse. Le tableau suivant répertorie les raisons pour lesquelles GuardDuty Malware Protection for EC2 peut ne pas analyser les ressources. Le cas échéant, suivez les étapes proposées pour résoudre ces problèmes et analysez ces ressources la prochaine fois que GuardDuty Malware Protection for EC2 lancera une analyse des programmes malveillants. Les autres problèmes sont utilisés pour vous informer sur le cours des événements et ne sont pas exploitables.

Motifs de l'omission	Explication	Étapes proposées	
RESOURCE_NOT_FOUND	Le code <code>resourceArn</code> fourni pour lancer l'analyse des programmes malveillants à la demande n'a pas été trouvé dans votre AWS environnement.	Validez l' <code>resourceArn</code> de votre instance ou charge de travail de conteneur Amazon EC2, puis réessayez.	
ACCOUNT_INELIGIBLE	L'ID de AWS compte à partir duquel vous avez essayé de lancer une analyse des On-demand programmes malveillants n'est pas activé GuardDuty.	Vérifiez que cette option GuardDuty est activée pour ce AWS compte. Lorsque vous activez GuardDuty une nouvelle fonctionnalité Région AWS , la synchronisation peut	

Motifs de l'omission	Explication	Étapes proposées	
		prendre jusqu'à 20 minutes.	
UNSUPPORT ED_KEY_EN CRYPTION	<p>GuardDuty Malware Protection for EC2 prend en charge les volumes non chiffrés et chiffrés à l'aide d'une clé gérée par le client. Il ne prend pas en charge l'analyse des volumes EBS chiffrés à l'aide du chiffrement Amazon EBS.</p> <p>À l'heure actuelle, il existe une différence régionale pour laquelle cette raison de saut n'est pas applicable. Pour plus d'informations à ce sujet Régions AWS, consultez Region-spécific disponibilité des fonctionnalités.</p>	<p>Remplacez votre clé de chiffrement par une clé gérée par le client. Pour plus d'informations sur les types de chiffrement pris GuardDuty en charge, consultez Volumes Amazon EBS pris en charge pour l'analyse des programmes malveillants.</p>	

Motifs de l'omission	Explication	Étapes proposées	
EXCLUDED_BY_SCAN_SETTINGS	L'instance EC2 ou le volume EBS a été exclu lors de l'analyse des programmes malveillants. Il existe deux possibilités : soit la balise a été ajoutée à la liste d'inclusion, mais la ressource n'est pas associée à cette balise, soit la balise a été ajoutée à la liste d'exclusion et la ressource est associée à cette balise, soit la balise GuardDuty Excluded est définie sur true pour cette ressource.	Mettez à jour vos options d'analyse ou les balises associées à votre ressource Amazon EC2. Pour de plus amples informations, veuillez consulter Options d'analyse avec balises définies par l'utilisateur .	
UNSUPPORTED_VOLUME_SIZE	Le volume est supérieur à 2 048 Go.	Non exploitable.	
NO_VOLUME_S_ATTACHED	GuardDuty Malware Protection for EC2 a détecté l'instance dans votre compte, mais aucun volume EBS n'a été associé à cette instance pour poursuivre l'analyse.	Non exploitable.	
UNABLE_TO_SCAN	Il s'agit d'une erreur de service interne.	Non exploitable.	

Motifs de l'omission	Explication	Étapes proposées	
SNAPSHOT_ NOT_FOUND	Les instantanés créés à partir des volumes EBS et partagés avec le compte de service sont introuvables et GuardDuty Malware Protection for EC2 n'a pas pu poursuivre l'analyse.	Assurez-vous que CloudTrail les instantanés n'ont pas été supprimés intentionnellement.	
SNAPSHOT_ QUOTA_REACHED	Vous avez atteint le volume maximum autorisé d'instantanés pour chaque région. Cela empêche non seulement de retenir, mais également de créer d'autres instantanés.	Vous pouvez soit supprimer les anciens instantanés, soit demander une augmentation du quota. Vous pouvez consulter la limite par défaut pour les instantanés par région et la procédure à suivre pour demander une augmentation de quota sous Service Quotas dans le Guide de référence général AWS .	

Motifs de l'omission	Explication	Étapes proposées	
MAX_NUMBE R_OF_ATTA CHED_VOLU MES_REACHED	Plus de 11 volumes EBS ont été attachés à une instance EC2. GuardDuty Malware Protection for EC2 a analysé les 11 premiers volumes EBS, obtenus en les triant par ordre alphabétique. deviceName	Non exploitable.	

Motifs de l'omission	Explication	Étapes proposées	
UNSUPPORT ED_PRODUC T_CODE_TYPE	<p>GuardDuty peut scanner la majorité des instances avec <code>productCode</code> <code>asmarketplace</code> . Certaines instances de la place de marché peuvent ne pas être éligibles à la numérisation. GuardDuty ignorera ces cas et enregistrera la raison sous la forme <code>UNSUPPORT ED_PRODUC T_CODE_TYPE</code> . Ce support varie selon AWS GovCloud (US) les régions de Chine. Pour de plus amples informations, veuillez consulter Region-spécific disponibilité des fonctionnalités.</p> <p>Pour plus d'informations, consultez la section AMI payantes dans le guide de l'utilisateur Amazon EC2. Pour plus d'informations sur <code>productCode</code> , veuillez consulter ProductCode dans</p>	Non exploitable.	

Motifs de l'omission	Explication	Étapes proposées	
	la Référence API d'Amazon EC2.		

Signalement des faux positifs dans Malware Protection for EC2

GuardDuty La protection contre les programmes malveillants pour les scans EC2 peut identifier un fichier inoffensif de votre instance Amazon EC2 ou de votre charge de travail de conteneur comme étant malveillant ou dangereux. Pour améliorer votre expérience avec Malware Protection for EC2 et le GuardDuty service, vous pouvez signaler des résultats faussement positifs si vous pensez qu'un fichier identifié comme étant malveillant ou dangereux lors d'une analyse ne contient pas réellement de logiciel malveillant.

Pour signaler un résultat d'analyse des programmes malveillants Amazon EC2 comme étant un faux positif

Pour lancer le processus, contactez Support. Procédez comme suit pour fournir des informations sur la ressource numérisée :

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Choisissez EC2 Malware Scans.
3. Choisissez une analyse pour voir son ID de résultat.
4. Communiquez l'ID de résultat. Vous devez également fournir le SHA-256 hachage du fichier. Cela est nécessaire pour garantir que GuardDuty Malware Protection for EC2 a reçu le bon fichier.
5. L' Support équipe vous fournira une URL présignée Amazon Simple Storage Service (Amazon S3) que vous pourrez utiliser pour télécharger le fichier et le hachage potentiellement malveillants. SHA-256 Pour plus d'informations sur les étapes de chargement de l'objet numérisé, consultez la section [Chargement d'objets avec des URL présignées](#) dans le guide de l'utilisateur Amazon S3.
6. Après avoir chargé le fichier, informez-en l' Support équipe.

Ils Support fourniront un accusé de réception après réception du fichier. Les membres GuardDuty de l'équipe de service analyseront votre demande et prendront les mesures

appropriées pour améliorer votre expérience avec Malware Protection for EC2 et le GuardDuty service. L' Support équipe continuera de fournir des mises à jour sur l'état de votre dossier. GuardDuty conserve votre objet S3 pendant 30 jours maximum.

Signaler le résultat de l'analyse d'un objet S3 comme faux positif dans Malware Protection for S3

Une protection contre les programmes malveillants pour l'analyse S3 peut identifier un objet comme potentiellement malveillant ou dangereux. Si vous pensez que l'objet S3 indiqué ne contient aucun logiciel malveillant, signalez le résultat de cette analyse de programmes malveillants comme un faux positif.

Vous pouvez envoyer un faux rapport positif même si vous utilisez Malware Protection for S3 de manière indépendante. Dans ce cas, n' GuardDuty est pas conçu pour générer un résultat. Pour plus d'informations sur la vérification de l'état du scan et de l'état des résultats, consultez [Surveillance des scans d'objets S3](#).

Pour signaler un résultat d'analyse des programmes malveillants d'un objet S3 comme étant un faux positif

Pour lancer le processus, contactez Support. Procédez comme suit pour fournir des informations sur l'objet S3 scanné :

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. En fonction de votre cas d'utilisation, choisissez les étapes appropriées :

Using Malware Protection for S3 with GuardDuty

1. Dans le volet de navigation, choisissez Conclusions.
2. Sur la page Résultats, sélectionnez le résultat faussement positif pour en afficher les détails.
3. En vérifiant les détails de la recherche, fournissez l'ID de recherche, la région, le nom du compartiment S3 protégé et la clé de l'objet scanné.

Dans les détails du chemin de l'élément, indiquez le hachage de l'objet. Cela est nécessaire pour s'assurer que le fichier reçu GuardDuty est correct.

Using Malware Protection for S3 independently

Indiquez le nom du compartiment S3 protégé, le nom de l'objet scanné et le Région AWS.

3. L' Support équipe vous fournira une URL présignée Amazon Simple Storage Service (Amazon S3) que vous pourrez utiliser pour télécharger le fichier et le hachage potentiellement malveillants. Pour plus d'informations sur les étapes de chargement de l'objet numérisé, consultez la section [Chargement d'objets avec des URL présignées](#) dans le guide de l'utilisateur Amazon S3.
4. Après avoir chargé l'objet S3, informez l' Support équipe.

Ils Support fourniront un accusé de réception de l'objet. Les membres de l'équipe de GuardDuty service analyseront votre envoi et prendront les mesures appropriées pour améliorer votre expérience avec Malware Protection for S3 et le GuardDuty service. L' Support équipe continuera de fournir des mises à jour sur l'état de votre dossier. GuardDuty conserve votre objet S3 pendant 30 jours maximum.

Signalement de faux positifs dans Malware Protection for Backup

Pour améliorer votre expérience avec GuardDuty Malware Protection for Backup, vous pouvez signaler des faux positifs et des faux négatifs potentiels.

Pour signaler un faux positif ou un faux négatif potentiel identifié dans Malware Protection for Backup

Pour lancer le processus, contactez Support. Procédez comme suit pour fournir des informations sur la ressource numérisée :

1. Connectez-vous à la GuardDuty console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Choisissez Analyses des logiciels malveillants.
3. Choisissez une analyse pour voir son ID de résultat.
4. Communiquez l'ID de résultat. Vous devez également fournir le SHA-256 hachage du fichier. Cela est nécessaire pour s'assurer que le fichier reçu GuardDuty est correct. Veuillez également indiquer la région d'où vous allez fournir l'échantillon.
5. L' Support équipe vous fournira une URL présignée Amazon Simple Storage Service (Amazon S3) que vous utiliserez pour télécharger le fichier et le hachage potentiellement malveillants.

SHA-256 Pour plus d'informations sur les étapes de téléchargement de la ressource numérisée, consultez la section [Chargement d'objets avec des URL présignées](#) dans le guide de l'utilisateur Amazon S3.

6. Après avoir chargé le fichier, informez-en l' Support équipe.

Ils Support fourniront un accusé de réception après réception du fichier. Les membres GuardDuty de l'équipe de service analyseront votre demande et prendront les mesures appropriées pour améliorer votre expérience avec Malware Protection for EC2. L' Support équipe continuera de fournir des mises à jour sur l'état de votre dossier. GuardDuty conserve votre objet S3 pendant 30 jours maximum.

Corriger les problèmes de GuardDuty sécurité détectés

Amazon GuardDuty génère des [résultats](#) qui indiquent des problèmes de sécurité potentiels associés à une détection GuardDuty fondamentale des menaces et à des plans de protection dédiés. Les sections suivantes décrivent les étapes de correction recommandées pour ces scénarios. S'il existe d'autres scénarios de remédiation, ils seront décrits dans les descriptions de chaque type de constatation. Vous pouvez accéder aux informations complètes sur un type de résultat en le sélectionnant dans le [tableau des types de résultat actifs](#).

Table des matières

- [Remédier à une instance Amazon EC2 potentiellement compromise](#)
- [Remédier à un compartiment S3 potentiellement compromis](#)
- [Remédier à un objet S3 potentiellement malveillant](#)
- [Remédier à un instantané EBS potentiellement compromis](#)
- [Remédier à une AMI EC2 potentiellement compromise](#)
- [Remédier à un point de restauration EC2 potentiellement compromis](#)
- [Remédier à un point de restauration S3 potentiellement compromis](#)
- [Remédier à un cluster ECS potentiellement compromis](#)
- [Remédier aux failles potentiellement compromises AWS informations d'identification](#)
- [Remédier à un conteneur autonome potentiellement compromis](#)
- [Corriger les résultats de la protection EKS](#)
- [Correction des résultats de la surveillance d'exécution](#)
- [Corriger une base de données potentiellement compromise](#)
- [Corriger une fonction Lambda potentiellement compromise](#)

Remédier à une instance Amazon EC2 potentiellement compromise

Lors de GuardDuty la [génération de types de recherche indiquant des ressources Amazon EC2 potentiellement compromises](#), votre ressource sera alors Instance. Les types de découvertes potentiels peuvent être [Types de résultat EC2GuardDuty Types de recherche liés à la surveillance du temps](#), ou [Protection contre les programmes malveillants pour les types de détection EC2](#). Si

le comportement à l'origine de la découverte était attendu dans votre environnement, pensez à l'utiliser [Règles de suppression](#).

Effectuez les étapes suivantes pour corriger l'instance Amazon EC2 potentiellement compromise :

1. Identifiez l'instance Amazon EC2 potentiellement compromise

Recherchez dans l'instance potentiellement compromise des programmes malveillants et supprimez ceux qui sont détectés. Vous pouvez utiliser [On-demand analyse des logiciels malveillants dans GuardDuty](#) pour identifier les logiciels malveillants dans l'instance EC2 potentiellement compromise, ou consulter [AWS Marketplace](#) pour vérifier s'il existe des produits partenaires utiles afin d'identifier et de supprimer les logiciels malveillants.

2. Isolez l'instance Amazon EC2 potentiellement compromise

Si possible, suivez les étapes suivantes pour isoler l'instance potentiellement compromise :

1. Créez un groupe de sécurité dédié à l'isolation. Un groupe de sécurité d'isolation ne doit disposer que d'un accès entrant et sortant à partir d'adresses IP spécifiques. Assurez-vous qu'aucune règle entrante ou sortante n'autorise le trafic pour. 0.0.0.0/0 (0-65535)
2. Associez le groupe de sécurité Isolation à cette instance.
3. Supprimez toutes les associations de groupes de sécurité autres que le groupe de sécurité Isolation nouvellement créé de l'instance potentiellement compromise.

Note

Les connexions suivies existantes ne seront pas interrompues en raison de la modification des groupes de sécurité. Seul le trafic futur sera effectivement bloqué par le nouveau groupe de sécurité.

Pour plus d'informations sur le blocage du trafic supplémentaire provenant de connexions existantes suspectes, voir [Appliquer les NACL en fonction du réseau IoT pour empêcher tout trafic supplémentaire](#) dans le manuel de réponse aux incidents.

3. Identifiez la source de l'activité suspecte.

Si un logiciel malveillant est détecté, identifiez et arrêtez l'activité potentiellement non autorisée sur votre instance EC2 en fonction du type de résultat dans votre compte. Cela peut nécessiter des actions telles que la fermeture de tous les ports ouverts, la modification des stratégies d'accès et la mise à niveau des applications pour corriger les vulnérabilités.

Si vous ne parvenez pas à identifier et à arrêter toute activité non autorisée sur votre instance EC2 potentiellement compromise, nous vous recommandons de mettre fin à l'instance EC2 compromise et de la remplacer par une nouvelle instance si nécessaire. Les ressources supplémentaires suivantes vous permettent de sécuriser vos instances EC2 :

- Section Sécurité et réseau de [Bonnes pratiques pour Amazon EC2](#).
- [Groupes de sécurité Amazon EC2 pour les instances Linux](#).
- [Sécurité dans Amazon EC2](#)
- [Conseils pour sécuriser vos instances EC2 \(Linux\)](#).
- [AWS bonnes pratiques en matière de sécurité](#)
- [AWS Guide technique de réponse aux incidents de sécurité](#).

4. Parcourir AWS re:Post

Consultez cette page [AWS re:Post](#) pour obtenir de l'aide supplémentaire.

5. Soumission d'une demande de support technique

Si vous êtes abonné à un package Premium Support, vous pouvez soumettre une demande de [support technique](#).

Remédier à un compartiment S3 potentiellement compromis

Une fois GuardDuty généré [GuardDuty Types de détection de la protection S3](#), il indique que vos compartiments Amazon S3 ont été compromis. Si le comportement à l'origine de la découverte était attendu dans votre environnement, envisagez de le créer [Règles de suppression](#). Si ce comportement n'était pas attendu, suivez ces étapes recommandées pour corriger un compartiment Amazon S3 potentiellement compromis dans votre AWS environnement :

1. Identifiez la ressource S3 potentiellement compromise.

Une GuardDuty recherche pour S3 indiquera le compartiment S3 associé, son Amazon Resource Name (ARN) et son propriétaire dans les détails de la recherche.

2. Identifiez la source de l'activité suspecte et l'appel d'API utilisé.

L'appel d'API utilisé est répertorié en tant qu'API dans les détails d'un résultat. La source sera un principal IAM (rôle IAM, utilisateur ou compte) et les informations d'identification seront répertoriées dans le résultat. Selon le type de source, l'adresse IP distante ou les informations

sur le domaine source seront disponibles et peuvent vous aider à déterminer si la source était autorisée. Si la découverte impliquait des informations d'identification provenant d'une instance Amazon EC2, les informations relatives à cette ressource seront également incluses.

3. Déterminez si la source de l'appel était autorisée à accéder à la ressource identifiée.

Prenons l'exemple suivant :

- Si un utilisateur IAM était impliqué, est-il possible que ses informations d'identification aient été potentiellement compromises ? Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).
- Si une API a été invoquée par un principal qui n'a jamais invoqué ce type d'API, cette source a-t-elle besoin d'autorisations d'accès pour cette opération ? Les autorisations du compartiment peuvent-elles être davantage restreintes ?
- Si l'accès a été détecté à partir du nom d'utilisateur ANONYMOUS_PRINCIPAL avec le type d'utilisateur de AWSAccount, cela indique que le compartiment est public et qu'il a été consulté. Ce compartiment doit-il être public ? Si ce n'est pas le cas, veuillez consulter les recommandations de sécurité ci-dessous pour découvrir des solutions alternatives au partage des ressources S3.
- Si l'accès a eu lieu par le biais d'un appel PreflightRequest réussi constaté à partir du nom d'utilisateur ANONYMOUS_PRINCIPAL avec le type d'utilisateur AWSAccount, cela indique que le compartiment dispose d'une stratégie de partage des ressources entre origines multiples (CORS) définie. Ce compartiment doit-il être doté d'une stratégie CORS ? Dans le cas contraire, assurez-vous que le compartiment n'a pas été rendu public par inadvertance et veuillez consulter les recommandations de sécurité ci-dessous pour trouver des solutions alternatives au partage des ressources S3. Pour plus d'informations sur CORS, veuillez consulter la section [Utilisation du partage des ressources entre origines multiples \(CORS\)](#) du Guide de l'utilisateur S3.

4. Déterminez si le compartiment S3 contient des données sensibles.

Utilisez [Amazon Macie](#) pour déterminer si le compartiment S3 contient des données sensibles, telles que des données d'identification personnelle (PII), des données financières ou des informations d'identification. Si la découverte automatique des données sensibles est activée pour votre compte Macie, examinez les détails du compartiment S3 pour mieux comprendre son contenu. Si cette fonctionnalité est désactivée pour votre compte Macie, nous vous recommandons de l'activer pour accélérer votre évaluation. Vous pouvez également créer et exécuter une tâche de découverte de données sensibles pour inspecter les objets du

compartiment S3 afin de détecter des données sensibles. Pour plus d'informations, veuillez consulter [Découverte de données sensibles avec Macie](#) (langue française non garantie).

Si l'accès a été autorisé, vous pouvez ignorer le résultat. La <https://console.aws.amazon.com/guardduty/> console vous permet de définir des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si vous déterminez que vos données S3 ont été exposées ou ont été consultées par une personne non autorisée, consultez les recommandations de sécurité S3 suivantes pour renforcer les autorisations et restreindre l'accès. Les solutions de correction appropriées dépendent des besoins de votre environnement spécifique.

Recommandations basées sur les besoins spécifiques d'accès au compartiment S3

La liste suivante fournit des recommandations en fonction des besoins spécifiques en matière d'accès au compartiment Amazon S3 :

- Pour limiter de manière centralisée l'accès public à l'utilisation de vos données S3, S3 bloque l'accès public. Les paramètres de blocage de l'accès public peuvent être activés pour les points d'accès, les compartiments et les AWS comptes via quatre paramètres différents afin de contrôler la granularité de l'accès. Pour plus d'informations, consultez la section [Bloquer les paramètres d'accès public](#) dans le guide de l'utilisateur Amazon S3.
- AWS Les politiques d'accès peuvent être utilisées pour contrôler la manière dont les utilisateurs IAM peuvent accéder à vos ressources ou à vos compartiments. Pour plus d'informations, consultez la section [Utilisation des politiques relatives aux compartiments et des politiques utilisateur](#) dans le guide de l'utilisateur Amazon S3.

Vous pouvez également utiliser des points de terminaison de cloud privé virtuel (VPC) avec des stratégies de compartiment S3 pour restreindre l'accès à des points de terminaison d'un VPC spécifiques. Pour plus d'informations, consultez la section [Contrôle de l'accès depuis les terminaux VPC à l'aide de politiques de compartiment](#) dans le guide de l'utilisateur Amazon S3.

- Pour autoriser temporairement l'accès à vos objets S3 à des entités approuvées extérieures à votre compte, vous pouvez créer une URL présignée via S3. Cet accès est créé à l'aide des informations d'identification de votre compte et, selon les informations d'identification utilisées, peut durer de

6 heures à 7 jours. Pour plus d'informations, consultez la section [Utilisation d'URL présignées pour télécharger et charger des objets](#) dans le guide de l'utilisateur Amazon S3.

- Pour les cas d'utilisation nécessitant le partage d'objets S3 entre différentes sources, vous pouvez utiliser les points d'accès S3 pour créer des ensembles d'autorisations qui limitent l'accès aux seuls utilisateurs de votre réseau privé. Pour plus d'informations, consultez [la section Gestion de l'accès aux ensembles de données partagés avec des points d'accès](#) dans le guide de l'utilisateur Amazon S3.
- Pour accorder en toute sécurité l'accès à vos ressources S3 à d'autres AWS comptes, vous pouvez utiliser une liste de contrôle d'accès (ACL). Pour plus d'informations, consultez la présentation de la liste de contrôle d'[accès \(ACL\)](#) dans le guide de l'utilisateur Amazon S3.

Pour plus d'informations sur les options de sécurité S3, consultez les meilleures pratiques de [sécurité pour Amazon S3](#) dans le guide de l'utilisateur Amazon S3.

Remédier à un objet S3 potentiellement malveillant

Une fois GuardDuty généré [Protection contre les programmes malveillants pour le type de recherche S3](#), il indique qu'un objet récemment chargé dans votre compartiment Amazon S3 contient un logiciel malveillant. Le type de ressource est un objet S3.

Suivez les étapes recommandées suivantes pour corriger éventuellement le résultat généré :

1. Identifiez l'objet S3 potentiellement malveillant en vérifiant ce qui est `S3ObjectDetails` associé à la découverte.
2. Isolez l'objet S3 impacté. Si vous aviez activé le balisage au moment de l'activation de la protection contre les programmes malveillants pour S3 pour le compartiment Amazon S3 associé, vous GuardDuty devez avoir attribué une balise malveillante à cet objet. Utilisez le contrôle d'accès basé sur les balises (TBAC) pour restreindre l'accès à cet objet S3. Pour de plus amples informations, veuillez consulter [Utilisation du contrôle d'accès basé sur des balises \(TBAC\)](#).

Sinon, si vous n'avez plus besoin de cet objet, vous pouvez également choisir de le supprimer ou de le déplacer vers un compartiment S3 isolé. Pour plus d'informations sur les considérations relatives à la suppression d'un objet S3, consultez [la section Supprimer des objets](#) dans le guide de l'utilisateur Amazon S3.

Remédier à un instantané EBS potentiellement compromis

Quand GuardDuty génère un Execution:EC2/MaliciousFile ! Type de recherche d'instantané, il indique qu'un logiciel malveillant a été détecté dans un instantané Amazon EBS. Effectuez les étapes suivantes pour corriger le snapshot potentiellement compromis :

1. Identifiez le snapshot potentiellement compromis

1. Identifiez le snapshot potentiellement compromis. La GuardDuty recherche d'un instantané EBS répertorie l'ID du cliché concerné, son Amazon Resource Name (ARN) et les détails de l'analyse des programmes malveillants associés dans les détails de la recherche.
2. Consultez les détails des points de restauration à l'aide de la commande suivante :

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789 --recovery-point-arn "arn:aws:ec2:us-east-1::snapshot/snap-abcdef01234567890"
```

2. Restreindre l'accès à l'instantané compromis

Passez en revue et modifiez les politiques d'accès au coffre-fort de sauvegarde pour restreindre l'accès aux points de restauration et suspendre toutes les tâches de restauration automatisées susceptibles d'utiliser cet instantané.

1. Passez en revue les autorisations de partage actuelles :

```
aws ec2 describe-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission
```

2. Supprimer l'accès à un compte spécifique :

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission --operation-type remove --user-ids 111122223333
```

3. Pour des options CLI supplémentaires, consultez la documentation de la CLI [modify-snapshot-attribute](#).

3. Prendre des mesures correctives

- Avant de procéder à la suppression, assurez-vous d'avoir identifié toutes les dépendances et de disposer de sauvegardes appropriées si nécessaire.

Remédier à une AMI EC2 potentiellement compromise

Quand GuardDuty génère un Execution:EC2/MaliciousFile ! Type de recherche AMI, il indique qu'un logiciel malveillant a été détecté dans une Amazon Machine Image (AMI). Effectuez les étapes suivantes pour corriger l'AMI potentiellement compromise :

1. Identifiez l'AMI potentiellement compromise

1. Une GuardDuty recherche pour les AMI indiquera l'ID d'AMI concerné, son Amazon Resource Name (ARN) et les détails de l'analyse des programmes malveillants associés dans les détails de la recherche.
2. Vérifiez l'image source de l'AMI :

```
aws ec2 describe-images --image-ids ami-021345abcdef6789
```

2. Restreindre l'accès aux ressources compromises

1. Passez en revue et modifiez les politiques d'accès au coffre-fort de sauvegarde afin de restreindre l'accès au point de restauration et de suspendre toutes les tâches de restauration automatisées susceptibles d'utiliser ce point de restauration.
2. Supprimer les autorisations des autorisations de l'AMI source

Consultez d'abord les autorisations existantes :

```
aws ec2 describe-image-attribute --image-id ami-abcdef01234567890 --attribute launchPermission
```

Supprimez ensuite les autorisations individuelles :

```
aws ec2 modify-image-attribute --image-id ami-abcdef01234567890 --launch-permission '{"Remove":[{"UserId":"111122223333"}]}'
```

Pour des options de CLI supplémentaires, voir [Partager une AMI avec des comptes spécifiques - Amazon Elastic Compute Cloud](#)

3. Si la source est une instance EC2, voir : [Remédier à une instance Amazon EC2 potentiellement compromise.](#)

3. Prendre des mesures correctives

- Avant de procéder à la suppression, assurez-vous d'avoir identifié toutes les dépendances et de disposer de sauvegardes appropriées si nécessaire.

Remédier à un point de restauration EC2 potentiellement compromis

Quand GuardDuty génère un `Execution:EC2/MaliciousFile ! RecoveryPoint` type de recherche, il indique qu'un logiciel malveillant a été détecté dans une ressource EC2 Recovery Point Backup. Effectuez les étapes suivantes pour corriger le point de restauration potentiellement compromis :

1. Identifiez le point de restauration EC2 potentiellement compromis

1. Une GuardDuty découverte pour EC2 Recovery Point indiquera son Amazon Resource Name (ARN) et les détails de l'analyse des programmes malveillants associés dans les détails de la recherche :

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
--recovery-point-arn "arn:aws:backup:us-east-1:111122223333:recovery-
point:a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"
```

2. Consultez les détails de la restauration pour rechercher l'image source :

```
aws backup get-recovery-point-restore-metadata --backup-vault-
name 021345abcdef6789 --recovery-point-arn "arn:aws:backup:us-
east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"
```

2. Restreindre l'accès aux ressources compromises

- Passez en revue et modifiez les politiques d'accès au coffre-fort de sauvegarde afin de restreindre l'accès au point de restauration et de suspendre toutes les tâches de restauration automatisées susceptibles d'utiliser ce point de restauration. Si votre environnement utilise le balisage des ressources, balisez le point de restauration de manière appropriée pour indiquer qu'il fait l'objet d'une enquête et envisagez de suspendre les sauvegardes planifiées si nécessaire.

Exemple :

```
aws backup tag-resource --resource-arn arn:aws:backup:us-east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --tags Investigation=Malware,DoNotDelete=True
```

3. Prendre des mesures correctives

- Avant de procéder à la suppression, assurez-vous d'avoir identifié toutes les dépendances et de disposer de sauvegardes appropriées si nécessaire.

Remédier à un point de restauration S3 potentiellement compromis

Quand GuardDuty génère un Execution:S3/MaliciousFile ! RecoveryPoint type de recherche, il indique qu'un logiciel malveillant a été détecté dans une ressource S3 Recovery Point Backup. Effectuez les étapes suivantes pour corriger le point de restauration potentiellement compromis :

1. Identifiez le point de restauration S3 potentiellement compromis

1. Une GuardDuty recherche pour les points de restauration S3 répertorie l'ARN du point de restauration concerné, le nom du coffre de sauvegarde et les détails de l'analyse des programmes malveillants associés dans les détails de la recherche.
2. Passez en revue les détails des points de récupération :

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789  
--recovery-point-arn arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef01234567890
```

2. Restreindre l'accès aux ressources compromises

- Passez en revue et modifiez les politiques d'accès au coffre-fort de sauvegarde afin de restreindre l'accès au point de restauration et de suspendre toutes les tâches de restauration automatisées susceptibles d'utiliser ce point de restauration. Si votre environnement utilise le balisage des ressources, balisez le point de restauration de manière appropriée pour indiquer qu'il fait l'objet d'une enquête et envisagez de suspendre les sauvegardes planifiées si nécessaire.

Exemple :

```
aws backup tag-resource --resource-arn arn:aws:backup:us-east-1:111122223333:recovery-point:abcdef01234567890 --  
tags Investigation=Malware,DoNotDelete=True
```

Pour plus de détails, voir : référence des commandes CLI [tag-resource](#)

3. Prendre des mesures correctives

- Avant de procéder à la suppression, assurez-vous d'avoir identifié toutes les dépendances et de disposer de sauvegardes appropriées si nécessaire.

Remédier à un cluster ECS potentiellement compromis

La découverte d'un cluster ECS potentiellement compromis indique qu'une activité suspecte ou malveillante a été détectée dans votre environnement Amazon ECS. Cela peut inclure un accès non autorisé, l'exécution de programmes malveillants ou tout autre comportement malveillant mettant en danger vos charges de travail de conteneurs.

Suivez ces étapes pour corriger un cluster Amazon ECS potentiellement compromis :

1. Identifier le cluster ECS potentiellement compromis et la menace détectée (résultats)

Les détails du cluster ECS concerné sont répertoriés dans le panneau GuardDuty des détails de la recherche.

2. Evaluer la source de threat/malware

Vérifiez la présence de logiciels malveillants dans les images des conteneurs. Si un logiciel malveillant est détecté, vérifiez l'image du conteneur utilisée. Permet [ListTasks](#) d'identifier toutes les autres tâches en cours d'exécution qui utilisent la même image potentiellement compromise.

3. Isolez les tâches concernées

Stoppez la menace en bloquant tout le trafic réseau (entrant et sortant) vers les tâches concernées. Cette isolation du réseau permet de prévenir toute attaque en cours en coupant toutes les connexions à la tâche compromise.

Remarque : Si vous déterminez que cette détection a été déclenchée par une expected/legitimate activité dans votre environnement, vous pouvez configurer une règle de suppression pour empêcher

l'apparition de résultats similaires. Pour plus d'informations, consultez [Règles de suppression dans GuardDuty](#).

Remédier aux failles potentiellement compromises AWS informations d'identification

Une fois GuardDuty généré [Types de résultat IAM](#), il indique que vos AWS informations d'identification ont été compromises. Le type de ressource potentiellement compromis est AccessKey.

Pour corriger les informations d'identification potentiellement compromises dans votre AWS environnement, effectuez les opérations suivantes :

1. Identifiez l'entité IAM potentiellement compromise et l'appel d'API utilisé.

L'appel d'API utilisé est répertorié en tant qu'API dans les détails d'un résultat. L'entité IAM (rôle IAM ou utilisateur) et ses informations d'identification seront répertoriées dans la section Ressource des détails de la recherche. Le type de l'entité IAM impliquée peut être déterminé par le champ User Type (Type d'utilisateur), le nom de l'entité IAM se trouvant dans le champ User name (Nom d'utilisateur). Le type de l'entité IAM impliquée dans le résultat peut également être déterminé par l'Access key ID (ID de clé d'accès) utilisé.

Pour les clés commençant par AKIA :

Ce type de clé est une information d'identification à long terme gérée par le client associée à un utilisateur IAM ou à un Utilisateur racine d'un compte AWS. Pour de plus amples informations sur la gestion des clés d'accès pour les utilisateurs IAM, veuillez consulter [Gestion des clés d'accès pour les utilisateurs IAM](#).

Pour les clés commençant par ASIA :

Ce type de clé est une information d'identification temporaire à court terme générée par AWS Security Token Service. Ces clés n'existent que depuis peu de temps et ne peuvent être ni affichées ni gérées dans la console AWS de gestion. Les rôles IAM utiliseront toujours des AWS STS informations d'identification, mais ils peuvent également être générés pour les utilisateurs IAM. Pour plus d'informations, AWS STS consultez [IAM : Informations d'identification de sécurité temporaires](#).

Si un rôle a été utilisé, le champ Nom d'utilisateur contient des informations sur le nom du rôle utilisé. Vous pouvez déterminer comment la clé a été demandée AWS CloudTrail en examinant

l'-sessionIssuerélément de l'entrée du CloudTrail journal. Pour plus d'informations, voir [IAM et AWS STS informations dans CloudTrail](#).

2. Vérifiez les autorisations pour l'entité IAM.

Ouvrez la console IAM. Selon le type d'entité utilisé, choisissez l'onglet Utilisateurs ou Rôles et localisez l'entité concernée en saisissant le nom identifié dans le champ de recherche. Utilisez les onglets Permission et Access Advisor pour vérifier les autorisations effectives pour cette entité.

3. Déterminez si les informations d'identification de l'entité IAM ont été utilisées de manière légitime.

Contactez l'utilisateur des informations d'identification pour déterminer si l'activité était intentionnelle.

Recherchez par exemple si l'utilisateur a effectué les actions suivantes :

- A invoqué l'opération d'API répertoriée dans la GuardDuty découverte
- Appeler l'opération API au moment où elle est répertoriée dans le résultat GuardDuty
- Appeler l'opération API à partir de l'adresse IP répertoriée dans le résultat GuardDuty

Si cette activité constitue une utilisation légitime des AWS informations d'identification, vous pouvez ignorer la GuardDuty découverte. La <https://console.aws.amazon.com/guardduty/> console vous permet de définir des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

Si vous ne pouvez pas confirmer si cette activité constitue une utilisation légitime, cela peut être dû à la compromission d'une clé d'accès spécifique, à savoir les informations de connexion de l'utilisateur IAM, ou peut-être la totalité. Compte AWS Si vous pensez que vos informations d'identification ont été compromises, consultez les informations contenues dans [My Compte AWS may be compromise](#) pour remédier à ce problème.

Remédier à un conteneur autonome potentiellement compromis

Lors de GuardDuty la [génération de types de recherche indiquant un conteneur potentiellement compromis](#), votre type de ressource sera Conteneur. Si le comportement à l'origine de la découverte était attendu dans votre environnement, pensez à l'utiliser [Règles de suppression](#).

Pour corriger les informations d'identification potentiellement compromises dans votre AWS environnement, effectuez les opérations suivantes :

1. Isolez le contenant potentiellement compromis

Les étapes suivantes vous aideront à identifier la charge de travail des conteneurs potentiellement malveillante :

- Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
- Sur la page Résultats, choisissez le résultat correspondant pour afficher le panneau des résultats.
- Dans le panneau des résultats, sous la section Ressource concernée, vous pouvez voir l'ID et le nom du conteneur.

Isolez ce conteneur des autres charges de travail de conteneur.

2. Mise en pause du conteneur

Suspendez tous les processus dans votre conteneur.

Pour plus d'informations sur la congélation de votre contenant, voir [Suspendre un contenant](#).

Arrêtez le contenant.

Si l'étape ci-dessus échoue et que le conteneur ne se suspend pas, arrêtez son exécution. Si vous avez activé cette [Conservation des instantanés](#) fonctionnalité, les instantanés de vos volumes EBS contenant des programmes malveillants GuardDuty seront conservés.

Pour plus d'informations sur l'arrêt du conteneur, voir [Arrêter un conteneur](#).

3. Évaluation de la présence de logiciels malveillants

Évaluez si un logiciel malveillant se trouvait dans l'image du conteneur.

Si l'accès a été autorisé, vous pouvez ignorer le résultat. La <https://console.aws.amazon.com/guardduty/> console vous permet de définir des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. La GuardDuty console vous permet de définir des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter [Règles de suppression dans GuardDuty](#).

Corriger les résultats de la protection EKS

Amazon GuardDuty génère des [résultats](#) qui indiquent des problèmes de sécurité potentiels de Kubernetes lorsque la protection EKS est activée pour votre compte. Pour de plus amples

informations, veuillez consulter [Protection EKS](#). Les sections suivantes décrivent les étapes de correction recommandées pour ces scénarios. Les mesures correctives spécifiques sont décrites dans l'entrée correspondant à ce type de résultat spécifique. Vous pouvez accéder aux informations complètes sur un type de résultat en le sélectionnant dans le [tableau des types de résultat actifs](#).

Si l'un des types de détection d'EKS Protection a été généré de manière inattendue, vous pouvez envisager de l'ajouter [Règles de suppression dans GuardDuty](#) pour éviter de futures alertes.

Différents types d'attaques et de problèmes de configuration peuvent déclencher les résultats d'GuardDuty EKS Protection. Ce guide vous aide à identifier les causes profondes des GuardDuty résultats concernant votre cluster et présente des conseils de remédiation appropriés. Les principales causes à l'origine des découvertes de GuardDuty Kubernetes sont les suivantes :

- [Problèmes de configuration potentiels](#)
- [Remédier aux utilisateurs de Kubernetes potentiellement compromis](#)
- [Remédier aux pods Kubernetes potentiellement compromis](#)
- [Remédier aux nœuds Kubernetes potentiellement compromis](#)
- [Corriger les images de conteneurs potentiellement compromises](#)

Note

Avant la version 1.14 de Kubernetes, le `system:unauthenticated` groupe était associé à `system:discovery` et par défaut, `system:basic-user` ClusterRoles. Cela peut autoriser un accès involontaire de la part d'utilisateurs anonymes. Les mises à jour de cluster ne révoquent pas ces autorisations, ce qui signifie que même si vous avez mis à jour votre cluster vers la version 1.14 ou ultérieure, elles peuvent toujours être en place. Nous vous recommandons de dissocier ces autorisations du groupe `system:unauthenticated`. Pour plus d'informations sur la suppression de ces autorisations, consultez la section [Sécuriser les clusters Amazon EKS avec les meilleures pratiques](#) dans le guide de l'utilisateur Amazon EKS .

Problèmes de configuration potentiels

Si un résultat indique un problème de configuration, veuillez consulter la section sur la correction de ce résultat pour obtenir des conseils sur la résolution de ce problème particulier. Pour de plus

amples informations, veuillez consulter les types de résultat suivants qui indiquent des problèmes de configuration :

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- Toute découverte qui se termine par `SuccessfulAnonymousAccess`

Remédier aux utilisateurs de Kubernetes potentiellement compromis

Une GuardDuty découverte peut indiquer la présence d'un utilisateur Kubernetes compromis lorsqu'un utilisateur identifié dans la découverte a effectué une action d'API inattendue. Vous pouvez identifier l'utilisateur dans la section Détails de l'utilisateur Kubernetes des détails d'un résultat dans la console, ou dans les `resource.kubernetesDetails.kubernetesUserDetails` des résultats JSON. Ces détails de l'utilisateur incluent `user name`, `uid` et les groupes Kubernetes auxquels l'utilisateur appartient.

Si l'utilisateur accédait à la charge de travail via une entité IAM, vous pouvez utiliser la section `Access Key details` pour identifier les détails d'un utilisateur ou d'un rôle IAM. Consultez les types d'utilisateur suivants et leurs conseils en matière de correction.

Note

Vous pouvez utiliser Amazon Detective pour étudier plus en détail l'utilisateur ou le rôle IAM identifié dans le résultat. Lorsque vous consultez les détails de la découverte dans GuardDuty la console, choisissez `Investiguer` dans Detective. Sélectionnez ensuite un AWS utilisateur ou un rôle parmi les éléments de la liste pour l'étudier dans Detective.

Built-in Kubernetes admin : utilisateur par défaut attribué par Amazon EKS à l'identité IAM qui a créé le cluster. Ce type d'utilisateur est identifié par le nom d'utilisateur `kubernetes-admin`.

Pour révoquer l'accès d'un administrateur Kubernetes intégré :

- Identifiez le `userType` dans la section `Access Key details`.
 - Si le `userType` est `Rôle` et que le rôle appartient à un rôle d'instance EC2 :

- Identifiez cette instance, puis suivez les instructions fournies dans [Remédier à une instance Amazon EC2 potentiellement compromise](#).
- Si le `userType` est Utilisateur ou un rôle assumé par un utilisateur :
 1. [Effectuez une rotation de la clé d'accès](#) de cet utilisateur.
 2. Effectuez une rotation de tous les secrets auxquels l'utilisateur avait accès.
 3. Consultez les informations contenues dans [My Compte AWS may be compromise](#) pour plus de détails.

Utilisateur authentifié OIDC : utilisateur auquel l'accès a été accordé par un fournisseur OIDC. Généralement, le nom d'utilisateur OIDC est une adresse e-mail. Vous pouvez vérifier si votre cluster utilise OIDC avec la commande suivante : `aws eks list-identity-provider-configs --cluster-name your-cluster-name` .

Pour révoquer l'accès d'un utilisateur authentifié OIDC :

1. Effectuez une rotation des informations d'identification de cet utilisateur dans le fournisseur OIDC.
2. Effectuez une rotation de tous les secrets auxquels l'utilisateur avait accès.

AWS Utilisateur ConfigMap défini par `-Auth` : utilisateur IAM auquel l'accès a été accordé via un `-auth`. AWS ConfigMap Pour plus d'informations, consultez [la section Gestion des utilisateurs ou des rôles IAM pour votre cluster](#) dans le guide de l'utilisateur Amazon EKS. Vous pouvez consulter les autorisations à l'aide de la commande suivante : `kubectl edit configmaps aws-auth --namespace kube-system`

Pour révoquer l'accès d'un AWS ConfigMap utilisateur :

1. Utilisez la commande suivante pour ouvrir le ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifiez le rôle ou l'entrée utilisateur dans la section `MapRoles` ou `MapUsers` avec le même nom d'utilisateur que celui indiqué dans la section des informations utilisateur Kubernetes de votre recherche. GuardDuty Consultez l'exemple suivant, où l'utilisateur administrateur a été identifié dans un résultat.

```
apiVersion: v1
data:
  mapRoles: |
```

```

- rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE306UCF
  user name: system:node:EC2_PrivateDNSName
  groups:
    - system:bootstrappers
    - system:nodes
mapUsers: |
- userarn: arn:aws:iam::123456789012:user/admin
  username: admin
  groups:
    - system:masters
- userarn: arn:aws:iam::111122223333:user/ops-user
  username: ops-user
  groups:
    - system:masters

```

3. Supprimez cet utilisateur du ConfigMap. Consultez l'exemple suivant où l'utilisateur administrateur a été supprimé.

```

apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE306UCF
      username: system:node:{EC2PrivateDNSName}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters

```

4. Si le userType est Utilisateur ou un rôle assumé par un utilisateur :
 - a. [Effectuez une rotation de la clé d'accès](#) de cet utilisateur.
 - b. Effectuez une rotation de tous les secrets auxquels l'utilisateur avait accès.
 - c. Consultez les informations de [Mon AWS compte qui peuvent être compromises](#) pour plus de détails.

Si le résultat ne comporte pas de section `resource.accessKeyDetails`, l'utilisateur est un compte de service Kubernetes.

Compte de service : le compte de service fournit une identité aux pods et peut être identifié par un nom d'utilisateur au format suivant : `system:serviceaccount:namespace:service_account_name`.

Pour révoquer l'accès à un compte de service :

1. Effectuez une rotation des informations d'identification du compte de service.
2. Consultez les instructions relatives à la compromission du pod dans la section suivante.

Remédier aux pods Kubernetes potentiellement compromis

Lorsque GuardDuty les détails d'un module ou d'une ressource de charge de travail sont spécifiés dans la `resource.kubernetesDetails.kubernetesWorkloadDetails` section, ce module ou cette ressource de charge de travail a été potentiellement compromis. Une GuardDuty découverte peut indiquer qu'un seul pod a été compromis ou que plusieurs pods ont été compromis par le biais d'une ressource de niveau supérieur. Consultez les scénarios de compromission suivants pour savoir comment identifier le ou les pods compromis.

Pods compromis individuels

Si le champ `type` dans la section `resource.kubernetesDetails.kubernetesWorkloadDetails` est `pods`, le résultat identifie un seul pod. Le champ de nom est le `name` des pods et le champ `namespace` est son espace de noms.

Pour plus d'informations sur l'identification du nœud de travail qui exécute les modules, consultez la section [Identifier les modules et le nœud de travail incriminés](#) dans le guide des meilleures pratiques d'Amazon EKS.

Pods compromis par le biais d'une ressource de charge de travail

Si le champ `type` de la section `resource.kubernetesDetails.kubernetesWorkloadDetails` identifie une ressource de charge de travail, comme un `Deployment`, il est probable que tous les pods de cette ressource de charge de travail aient été compromis.

Pour plus d'informations sur l'identification de tous les modules de la ressource de charge de travail et des nœuds sur lesquels ils s'exécutent, voir [Identifier les modules et les nœuds de](#)

[travail incriminés à l'aide du nom de la charge de travail](#) dans le guide des meilleures pratiques Amazon EKS.

Pods compromis par le biais d'un compte de service

Si une GuardDuty découverte identifie un compte de service dans la `resource.kubernetesDetails.kubernetesUserDetails` section, il est probable que les pods utilisant le compte de service identifié soient compromis. Le nom d'utilisateur indiqué par un résultat est un compte de service s'il a le format suivant : `system:serviceaccount:namespace:service_account_name`.

Pour plus d'informations sur l'identification de tous les pods à l'aide du compte de service et des nœuds sur lesquels ils s'exécutent, voir [Identifier les pods et les nœuds de travail incriminés à l'aide du nom du compte de service](#) dans le Guide des meilleures pratiques Amazon EKS.

Une fois que vous avez identifié tous les espaces compromis et les nœuds sur lesquels ils s'exécutent, consultez la section [Isoler l'espace en créant une politique réseau qui refuse tout le trafic entrant et sortant vers l'espace](#) dans le guide des meilleures pratiques Amazon EKS.

Pour remédier à un pod potentiellement compromis, procédez comme suit :

1. Identifiez la vulnérabilité qui a compromis les pods.
2. Mettez en œuvre le correctif pour cette vulnérabilité et démarrez de nouveaux pods de remplacement.
3. Supprimez les pods vulnérables.

Pour plus d'informations, consultez [Redéployer un pod ou une ressource de charge de travail compromis](#) dans le guide des meilleures pratiques Amazon EKS.

Si le nœud de travail s'est vu attribuer un rôle IAM qui permet aux Pods d'accéder à d'autres AWS ressources, supprimez ces rôles de l'instance pour éviter de nouveaux dommages dus à l'attaque. De même, si un rôle IAM a été attribué au pod, déterminez si vous pouvez supprimer les politiques IAM du rôle en toute sécurité sans affecter les autres charges de travail.

Corriger les images de conteneurs potentiellement compromises

Lorsqu'une GuardDuty découverte indique une compromission d'un pod, l'image utilisée pour lancer le pod peut être potentiellement malveillante ou compromise. GuardDuty les résultats identifient l'image du conteneur

`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` sur le terrain. Vous pouvez déterminer si l'image est malveillante en l'analysant afin de détecter des logiciels malveillants.

Pour corriger une image de conteneur potentiellement compromise, procédez comme suit :

1. Arrêtez immédiatement d'utiliser l'image et supprimez-la de votre référentiel d'images.
2. Identifiez tous les pods à l'aide de l'image potentiellement compromise.

Pour plus d'informations, consultez la section [Identifier les pods contenant des images et des nœuds de travail vulnérables ou compromis](#) dans le guide des meilleures pratiques Amazon EKS.

3. Isolez les pods potentiellement compromis, alternez les informations d'identification et collectez des données à des fins d'analyse. Pour plus d'informations, voir [Isoler l'espace en créant une politique réseau qui refuse tout trafic entrant et sortant vers l'espace](#) dans le Guide des meilleures pratiques Amazon EKS.
4. Supprimez tous les pods à l'aide de l'image potentiellement compromise.

Remédier aux nœuds Kubernetes potentiellement compromis

Une GuardDuty découverte peut indiquer une compromission de nœud si l'utilisateur identifié dans la découverte représente une identité de nœud ou si la découverte indique l'utilisation d'un conteneur privilégié.

L'identité de l'utilisateur est un composant master si le champ username a le format suivant : `system:node:node name`. Par exemple, `system:node:ip-192-168-3-201.ec2.internal`. Cela indique que l'adversaire a obtenu l'accès au nœud et qu'il utilise les informations d'identification du nœud pour communiquer avec le point de terminaison de l'API Kubernetes.

Un résultat indique l'utilisation d'un conteneur privilégié si un ou plusieurs conteneurs répertoriés dans le résultat a le champ de résultat `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext` défini sur `True`.

Pour remédier à un nœud potentiellement compromis, procédez comme suit :

1. Isolez le module, alternez ses informations d'identification et collectez des données à des fins d'analyse médico-légale.

Pour plus d'informations, voir [Isoler l'espace en créant une politique réseau qui refuse tout trafic entrant et sortant vers l'espace](#) dans le Guide des meilleures pratiques Amazon EKS.

2. Identifiez les comptes de service utilisés par tous les pods s'exécutant sur le nœud potentiellement compromis. Vérifiez leurs autorisations et effectuez une rotation des comptes de service, si nécessaire.
3. Mettez fin au nœud potentiellement compromis.

Correction des résultats de la surveillance d'exécution

Lorsque vous activez la surveillance du temps d'exécution pour votre compte, Amazon GuardDuty peut générer des informations [GuardDuty Types de recherche liés à la surveillance du temps](#) indiquant des problèmes de sécurité potentiels dans votre AWS environnement. Les problèmes de sécurité potentiels indiquent soit une instance Amazon EC2 compromise, soit une charge de travail de conteneur, soit un cluster Amazon EKS, soit un ensemble d'informations d'identification compromises dans votre AWS environnement. L'agent de sécurité surveille les événements d'exécution provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans les détails de recherche générés dans la GuardDuty console. La section suivante décrit les étapes de correction recommandées pour chaque type de ressource.

Instance

Si le type de ressource indiqué dans les détails du résultat est Instance, cela indique qu'une instance EC2 ou un nœud EKS est potentiellement compromis.

- Pour corriger un nœud EKS compromis, veuillez consulter [Remédier aux nœuds Kubernetes potentiellement compromis](#).
- Pour corriger une instance EC2 compromise, veuillez consulter [Remédier à une instance Amazon EC2 potentiellement compromise](#).

EKSCluster

Si le type de ressource indiqué dans les détails du résultat est EKSCluster, cela indique qu'un pod ou un conteneur dans un cluster EKS est potentiellement compromis.

- Pour corriger un pod compromis, veuillez consulter [Remédier aux pods Kubernetes potentiellement compromis](#).
- Pour corriger une image de conteneur compromise, veuillez consulter [Corriger les images de conteneurs potentiellement compromises](#).

ECSCluster

Si le type de ressource indiqué dans les détails de la recherche est ECSCluster, cela indique qu'une tâche ECS ou un conteneur à l'intérieur d'une tâche ECS est potentiellement compromis.

1. Identifier le cluster ECS concerné

La recherche GuardDuty Runtime Monitoring fournit les détails du cluster ECS dans le panneau de détails de la recherche ou dans la `resource.ecsClusterDetails` section du JSON de recherche.

2. Identifier la tâche ECS concernée

La recherche GuardDuty Runtime Monitoring fournit les détails de la tâche ECS dans le panneau de détails de la recherche ou dans la `resource.ecsClusterDetails.taskDetails` section du JSON de recherche.

3. Isolez la tâche concernée

Isolez la tâche concernée en refusant tout trafic entrant et sortant vers la tâche. Une règle interdisant tout trafic peut aider à stopper une attaque déjà en cours, en coupant toutes les connexions à la tâche.

4. Corrigez la tâche compromise

- a. Identifiez la vulnérabilité qui a compromis la tâche.
- b. Implémentez le correctif pour cette vulnérabilité et lancez une nouvelle tâche de remplacement.
- c. Arrêtez cette tâche vulnérable.

Container

Si le type de ressource indiqué dans les détails du résultat est Conteneur, cela indique qu'un conteneur autonome est potentiellement compromis.

- Pour remédier à cette situation, veuillez consulter [Remédier à un conteneur autonome potentiellement compromis](#).
- Si le résultat est généré sur plusieurs conteneurs à l'aide de la même image de conteneur, veuillez consulter [Corriger les images de conteneurs potentiellement compromises](#).
- Si le conteneur a accédé à l'hôte EC2 sous-jacent, ses informations d'identification d'instance associées ont peut-être été compromises. Pour de plus amples informations, veuillez consulter [Remédier aux failles potentiellement compromises AWS informations d'identification](#).
- Si un acteur potentiellement malveillant a accédé au nœud EKS ou à une instance EC2 sous-jacent, veuillez consulter la correction recommandée sous les onglets EKSCluster et Instance.

Correction des images de conteneur compromises

Lorsqu'une GuardDuty découverte indique une compromission de la tâche, l'image utilisée pour lancer la tâche peut être malveillante ou compromise. GuardDuty les résultats identifient l'image du conteneur `resource.ecsClusterDetails.taskDetails.containers.image` sur le terrain. Vous pouvez déterminer si l'image est malveillante en la recherchant.

Pour corriger une image de conteneur compromise

1. Arrêtez immédiatement d'utiliser l'image et supprimez-la de votre référentiel d'images.
2. Identifiez toutes les tâches qui utilisent cette image.
3. Arrêtez toutes les tâches qui utilisent l'image compromise. Mettez à jour leurs définitions de tâches afin qu'ils cessent d'utiliser l'image compromise.

Corriger une base de données potentiellement compromise

GuardDuty génère [Types de résultat de la protection RDS](#) qui indiquent un comportement de connexion potentiellement suspect et anormal chez vous une [Bases de données prises en charge](#) fois que vous l'avez activé [Protection RDS](#). L'activité de connexion RDS permet d' GuardDuty analyser et de profiler les menaces en identifiant les modèles inhabituels lors des tentatives de connexion.

 Note

Vous pouvez accéder aux informations complètes sur un type de résultat en le sélectionnant dans la [GuardDuty types de recherche actifs](#).

Suivez ces étapes recommandées pour corriger une base de données Amazon Aurora potentiellement compromise dans votre AWS environnement.

Rubriques

- [Correction d'une base de données potentiellement compromise avec des événements de connexion réussie](#)
- [Correction d'une base de données potentiellement compromise avec des événements de connexion échouée](#)
- [Corriger une base de données potentiellement compromise par une activité d'exfiltration anormale](#)
- [Corriger une base de données potentiellement compromise par une activité destructrice anormale](#)
- [Correction d'informations d'identification compromises](#)
- [Retreindre l'accès au réseau](#)

Correction d'une base de données potentiellement compromise avec des événements de connexion réussie

Les étapes recommandées ci-dessous peuvent vous aider à corriger une base de données Aurora potentiellement compromise qui présente un comportement inhabituel lié à des événements de connexion réussie.

1. Identifiez la base de données et l'utilisateur concernés.

Le GuardDuty résultat généré fournit le nom de la base de données affectée et les informations utilisateur correspondantes. Pour plus d'informations, consultez [Détails d'un résultat](#).

2. Vérifiez si ce comportement est attendu ou inattendu.

La liste suivante indique les scénarios potentiels susceptibles d'avoir entraîné GuardDuty la génération d'un résultat :

- Un utilisateur qui se connecte à sa base de données après une longue période.

- Un utilisateur qui se connecte à sa base de données de façon occasionnelle, par exemple un analyste financier qui se connecte chaque trimestre.
 - Un acteur potentiellement suspect impliqué dans une tentative de connexion réussie peut compromettre la base de données.
3. Commencez cette étape si le comportement est inattendu.
1. Restreindre l'accès à la base de données
- Limitez l'accès à la base de données pour les comptes suspects et la source de cette activité de connexion. Pour plus d'informations, consultez [Correction d'informations d'identification compromises](#) et [Restreindre l'accès au réseau](#).
2. Évaluez l'impact et déterminez quelles informations ont été consultées.
- Le cas échéant, veuillez consulter les journaux d'audit pour identifier les informations susceptibles d'avoir été consultées. Pour de plus amples informations, veuillez consulter [Surveillance des événements, des journaux et des flux dans un cluster de base de données Amazon Aurora](#) dans le Guide de l'utilisateur Amazon Aurora.
 - Déterminez si des informations sensibles ou protégées ont été consultées ou modifiées.

Correction d'une base de données potentiellement compromise avec des événements de connexion échouée

Les étapes recommandées ci-dessous peuvent vous aider à corriger une base de données Aurora potentiellement compromise qui présente un comportement inhabituel lié à des événements de connexion échouée.

1. Identifiez la base de données et l'utilisateur concernés.

Le GuardDuty résultat généré fournit le nom de la base de données affectée et les informations utilisateur correspondantes. Pour plus d'informations, consultez [Détails d'un résultat](#).

2. Identifiez la source des tentatives de connexion infructueuses.

Le GuardDuty résultat généré fournit l'adresse IP et l'organisation ASN (s'il s'agissait d'une connexion publique) dans la section Acteur du panneau de recherche.

Un système autonome est un groupe d'un ou de plusieurs préfixes IP (listes d'adresses IP accessibles sur un réseau) gérés par un ou plusieurs opérateurs réseau qui appliquent une stratégie de routage unique et clairement définie. Les opérateurs réseau ont besoin de numéros

de système autonomes (ASN) pour contrôler le routage au sein de leurs réseaux et pour échanger des informations de routage avec d'autres fournisseurs de services Internet (FSI).

3. Vérifiez que ce comportement est inattendu.

Vérifiez si cette activité représente une tentative d'obtenir un accès non autorisé supplémentaire à la base de données comme suit :

- Si la source est interne, vérifiez si une application est mal configurée et tente de se connecter à plusieurs reprises.
- S'il s'agit d'un acteur externe, vérifiez si la base de données correspondante est accessible au public ou si elle est mal configurée, ce qui permet à des acteurs malveillants potentiels de recourir à une attaque en force visant à obtenir les noms d'utilisateur courants.

4. Commencez cette étape si le comportement est inattendu.

1. Restreindre l'accès à la base de données

Limitez l'accès à la base de données pour les comptes suspects et la source de cette activité de connexion. Pour plus d'informations, consultez [Correction d'informations d'identification compromises](#) et [Restreindre l'accès au réseau](#).

2. Effectuez une analyse des causes profondes et déterminez les étapes qui ont potentiellement donné lieu à cette activité.

Configurez une alerte pour être averti lorsqu'une activité modifie une stratégie réseau et crée un état non sécurisé. Pour plus d'informations, veuillez consulter [Politiques de pare-feu dans AWS Network Firewall](#) dans le Guide du développeur AWS Network Firewall (langue française non garantie).

Corriger une base de données potentiellement compromise par une activité d'exfiltration anormale

Les étapes recommandées ci-dessous peuvent vous aider à remédier à une base de données Aurora potentiellement compromise qui présente un comportement inhabituel lié à des événements d'exfiltration de données.

1. Identifiez la base de données et l'utilisateur concernés.

Le GuardDuty résultat généré fournit le nom de la base de données affectée et les informations utilisateur correspondantes. Pour plus d'informations, consultez [Détails d'un résultat](#).

2. Identifiez l'étendue des données consultées.

Passez en revue les journaux d'activité des données RDS disponibles pour déterminer quelles tables et quelles lignes ont été consultées par l'utilisateur anormal pendant la période indiquée par le résultat. Évaluez la sensibilité des données potentiellement exfiltrées.

3. Vérifiez que ce comportement est inattendu.

Vérifiez si cette activité représente un comportement opérationnel légitime comme suit :

- Si la source est interne, vérifiez si une tâche ETL planifiée, un outil de reporting ou un processus de sauvegarde peuvent expliquer le volume élevé de requêtes.
- S'il s'agit d'un acteur externe ou d'un attribut de base de données invisible auparavant, vérifiez si les informations d'identification de base de données correspondantes peuvent avoir été exposées ou partagées en externe.
- Vérifiez si la combinaison du volume et des attributs invisibles (adresse IP, ASN, nom de l'application) correspond à un changement opérationnel connu.

4. Commencez cette étape si le comportement est inattendu.

Révoquez l'accès et alternez les informations d'identification.

Modifiez immédiatement le mot de passe de l'utilisateur de base de données concerné et révoquez les sessions actives. Si l'utilisateur dispose de privilèges élevés, limitez temporairement ses autorisations à la lecture seule ou supprimez complètement l'accès jusqu'à ce que l'enquête soit terminée.

5. Évaluez l'impact commercial.

Identifiez les données accessibles à l'utilisateur concerné, déterminez si des données sensibles ou réglementées (informations personnelles, financières, soins de santé) ont été potentiellement exfiltrées et suivez les procédures de notification des violations de données de votre organisation, le cas échéant.

6. Limitez l'accès au réseau.

Limitez l'accès à la base de données pour les comptes suspects et la source de cette activité. Placez la base de données dans un VPC privé si ce n'est déjà fait, et limitez les règles du groupe de sécurité pour autoriser le trafic provenant uniquement des sources nécessaires. Pour plus d'informations, consultez [Retreindre l'accès au réseau](#).

7. Effectuez une analyse des causes profondes et déterminez les étapes qui ont potentiellement donné lieu à cette activité.

Configurez une alerte pour être averti lorsqu'une activité modifie une stratégie réseau et crée un état non sécurisé. Pour plus d'informations, veuillez consulter [Politiques de pare-feu dans AWS Network Firewall](#) dans le Guide du développeur AWS Network Firewall (langue française non garantie).

Corriger une base de données potentiellement compromise par une activité destructrice anormale

Les étapes recommandées ci-dessous peuvent vous aider à remédier à une base de données Aurora potentiellement compromise qui présente un comportement inhabituel lié à des DROP événements DELETE ou à des destructions.

1. Identifiez la base de données et l'utilisateur concernés.

Le GuardDuty résultat généré fournit le nom de la base de données affectée et les informations utilisateur correspondantes. Pour plus d'informations, consultez [Détails d'un résultat](#).

2. Identifiez l'étendue des opérations destructrices.

Consultez les journaux d'activité des données RDS disponibles pour déterminer quelles tables, lignes ou objets de base de données ont été supprimés ou supprimés par l'utilisateur anormal pendant la période indiquée par le résultat. Déterminez si la perte de données est récupérable à partir de sauvegardes ou de snapshots existants.

3. Vérifiez que ce comportement est inattendu.

Vérifiez si cette activité représente un comportement opérationnel légitime comme suit :

- Si la source est interne, déterminez si une tâche de maintenance planifiée, un script de nettoyage ou un processus de migration peuvent prendre en compte les DROP opérations DELETE ou.
- S'il s'agit d'un acteur externe ou d'un attribut de base de données invisible auparavant, vérifiez si les informations d'identification de base de données correspondantes ont peut-être été exposées ou compromises.
- Vérifiez si la combinaison d'opérations destructrices et d'attributs invisibles (adresse IP, ASN, nom de l'application) correspond à un changement opérationnel connu.

4. Commencez cette étape si le comportement est inattendu.

Révoquez l'accès et alternez les informations d'identification.

Modifiez immédiatement le mot de passe de l'utilisateur de base de données concerné et révoquez les sessions actives. Supprimez les DELETE privilèges DROP et privilèges de l'utilisateur jusqu'à ce que l'enquête soit terminée afin d'empêcher toute destruction ultérieure des données.

5. Lancez la restauration des données.

Si la perte de données est confirmée, lancez une restauration instantanée à partir de sauvegardes automatisées ou à partir de l'instantané le plus récent. Pour Amazon Aurora, vous pouvez utiliser le backtrack pour rétablir la base de données à une époque antérieure à l'activité destructrice. Pour Amazon RDS, utilisez la restauration instantanée pour rétablir la situation à un point antérieur à l'événement.

6. Limitez l'accès au réseau et renforcez les autorisations.

Limitez l'accès à la base de données pour les comptes suspects et la source de cette activité. Placez la base de données dans un VPC privé si ce n'est déjà fait, et limitez les règles du groupe de sécurité pour autoriser le trafic provenant uniquement des sources nécessaires. Passez en revue les politiques IAM et les privilèges des utilisateurs de base de données pour appliquer l'accès au moindre privilège et activez la protection contre la suppression sur l'instance RDS si ce n'est déjà fait. Pour plus d'informations, consultez [Retreindre l'accès au réseau](#).

7. Effectuez une analyse des causes profondes et déterminez les étapes qui ont potentiellement donné lieu à cette activité.

Configurez une alerte pour être averti lorsqu'une activité modifie une stratégie réseau et crée un état non sécurisé. Pour plus d'informations, veuillez consulter [Politiques de pare-feu dans AWS Network Firewall](#) dans le Guide du développeur AWS Network Firewall (langue française non garantie).

Correction d'informations d'identification compromises

Une GuardDuty découverte peut indiquer que les informations d'identification d'utilisateur d'une base de données affectée ont été compromises lorsque l'utilisateur identifié dans la recherche a effectué une opération de base de données inattendue. Vous pouvez identifier l'utilisateur dans la section Détails de l'utilisateur de la base de données RDS dans le panneau de résultat de la console, ou dans les `resource.rdsDbUserDetails` des résultats JSON. Ces informations utilisateur incluent le nom d'utilisateur, l'application utilisée, la base de données consultée, la version SSL et la méthode d'authentification.

- Pour révoquer l'accès ou modifier les mots de passe pour des utilisateurs spécifiques impliqués dans le résultat, veuillez consulter [Sécurité avec Amazon Aurora MySQL](#) ou [Sécurité avec Amazon Aurora PostgreSQL](#) dans le Guide de l'utilisateur Amazon Aurora.
- Utilisez-le AWS Secrets Manager pour stocker en toute sécurité et faire automatiquement pivoter les secrets des bases de données Amazon Relational Database Service (RDS). Pour plus d'informations, veuillez consulter la rubrique [Didacticiels AWS Secrets Manager](#) dans le Guide de l'utilisateur AWS Secrets Manager .
- Utilisez l'authentification de base de données IAM pour gérer l'accès des utilisateurs de base de données sans avoir besoin de mots de passe. Pour de plus amples informations, veuillez consulter [Authentification de base de données IAM](#) dans le Guide de l'utilisateur Amazon Aurora.

Pour de plus amples informations, veuillez consulter [Bonnes pratiques en matière de sécurité pour Amazon Relational Database Service](#) dans le Guide de l'utilisateur Amazon RDS.

Retreindre l'accès au réseau

Une GuardDuty découverte peut indiquer qu'une base de données est accessible au-delà de vos applications ou du Virtual Private Cloud (VPC). Si l'adresse IP distante indiquée dans le résultat est une source de connexion inattendue, vérifiez les groupes de sécurité.

Une liste des groupes de sécurité attachés à la base de données est disponible sous Groupes de sécurité dans la <https://console.aws.amazon.com/rds/> console ou dans le JSON resource.rdsDbInstanceDetails.dbSecurityGroups des résultats. Pour de plus amples informations sur la configuration des groupes de sécurité, veuillez consulter [Contrôle d'accès par groupes de sécurité](#) dans le Guide de l'utilisateur Amazon RDS.

Si vous utilisez un pare-feu, limitez l'accès réseau à la base de données en reconfigurant les listes de contrôle d'accès réseau (NACL). Pour plus d'informations, veuillez consulter [Pare-feux dans AWS Network Firewall](#) dans le Guide du développeur AWS Network Firewall .

Corriger une fonction Lambda potentiellement compromise

Lors de GuardDuty la [Types de résultat de la protection Lambda](#) génération, votre fonction Lambda peut être compromise. Si l'activité GuardDuty à l'origine de ce résultat était attendue, vous pouvez envisager d'utiliser [Règles de suppression](#). Nous vous recommandons de suivre les étapes suivantes pour corriger une fonction Lambda compromise :

Pour corriger les résultats de la protection Lambda

1. Identifiez la version de la fonction Lambda potentiellement compromise.

Une GuardDuty recherche pour Lambda Protection fournit le nom, le nom de ressource Amazon (ARN), la version de la fonction et l'ID de révision associés à la fonction Lambda répertoriés dans les détails de la recherche.

2. Identifiez la source de l'activité potentiellement suspecte.
 - a. Examinez le code associé à la version de la fonction Lambda impliquée dans le résultat.
 - b. Examinez les bibliothèques et les couches importées de la version de la fonction Lambda impliquée dans le résultat.
 - c. Si vous avez activé [AWS Lambda les fonctions de numérisation avec Amazon Inspector](#), consultez les [résultats Amazon Inspector](#) associés à la fonction Lambda impliquée dans le résultat.
 - d. Passez en revue les AWS CloudTrail journaux pour identifier le principal responsable de la mise à jour de la fonction et assurez-vous que l'activité était autorisée ou attendue.
3. Corrigez la fonction Lambda potentiellement compromise.
 - a. Désactivez les déclencheurs d'exécution de la fonction Lambda impliqués dans le résultat. Pour de plus amples informations, veuillez consulter [DeleteFunctionEventInvokeConfig](#).
 - b. Examinez le code Lambda et mettez à jour les importations de bibliothèques et les [couches de fonctions Lambda](#) afin de supprimer les bibliothèques et les couches potentiellement suspects.
 - c. Atténuez les résultats Amazon Inspector liés à la fonction Lambda impliquée dans le résultat.

Surveillance de GuardDuty l'utilisation et estimation des coûts

GuardDuty fournit des mesures d'utilisation qui permettent de suivre le traitement des sources de données des plans de protection logs/events et des vCPU surveillés par GuardDuty Runtime au fil du temps.

Dans cette page :

- [Statistiques CloudWatch d'utilisation d'Amazon](#)
- [Comprendre GuardDuty l'utilisation](#)
- [Estimation des GuardDuty coûts](#)

Statistiques CloudWatch d'utilisation d'Amazon

GuardDuty publie des statistiques d'utilisation sur Amazon CloudWatch, ce qui vous permet de :

- Suivez l'utilisation réelle au fil du temps
- Créez des tableaux de bord et des alarmes personnalisés
- Exportez les données d'utilisation pour l'estimation des coûts dans AWS Pricing Calculator

GuardDuty les statistiques d'utilisation sont publiées en fonction de la configuration de votre compte :

- Tous les comptes (comptes autonomes, administrateurs délégués et membres) reçoivent des statistiques d'utilisation individuelles sur Amazon CloudWatch
- Les comptes d'administrateur délégué reçoivent en outre des statistiques d'utilisation agrégées pour l'ensemble de l'organisation.

GuardDuty les statistiques d'utilisation sont publiées sur Amazon CloudWatch dans les 24 heures.

Détails des métriques

GuardDuty publie les mesures Hourly d'utilisation suivantes sur Amazon CloudWatch sous l'AWS/GuardDuty espace de noms :

Plan de protection	Source de données	Nom de la métrique	Unité	Description
Détection fondamentale des menaces	CloudTrailEvents	AnalyzedCount	Nombre	Nombre d'événements CloudTrail de gestion analysés
Détection fondamentale des menaces	VPCFlowLogDNSLogEvents	AnalyzedBytes	Octets	Volume de journaux de flux VPC et de journaux DNS analysés
Protection EKS	KubernetesAuditLogs	AnalyzedCount	Nombre	Nombre d'événements du journal d'audit Amazon EKS analysés
Protection S3	S3DataEvents	AnalyzedCount	Nombre	Nombre d'événements de données S3 analysés
Surveillance d'exécution	RuntimeMonitoringEC2	Monitored VcpuHours	Compte (vCPU-Hours)	Heures du vCPU EC2 surveillées par Runtime Monitoring
Surveillance d'exécution	RuntimeMonitoringEKS	Monitored VcpuHours	Compte (vCPU-Hours)	Heures de vCPU Amazon EKS surveillées par Runtime Monitoring
Surveillance d'exécution	RuntimeMonitoringFargate	Monitored VcpuHours	Compte (vCPU-Hours)	Heures du vCPU Fargate surveillé

				es par Runtime Monitoring
Protection contre les programmes malveillants pour EC2	OnDemandEBSSnapshot	ScannedBytes	Octets	Volume de données instantanées EBS numérisées à la demande
Protection contre les programmes malveillants pour EC2	OnDemandEBSVolume	ScannedBytes	Octets	Volume de données de volume EBS numérisées à la demande
Protection contre les programmes malveillants pour EC2	MalwareProtectionEBS	ScannedBytes	Octets	Volume de données EBS analysées par Malware Protection
Protection RDS	RDS	MonitoredAcuHours	Compter (ACU-Hours)	Unités de capacité Amazon RDS Aurora surveillées
Protection RDS	RDS Limitless	MonitoredAcuHours	Compter (ACU-Hours)	Heures ACU Amazon RDS Aurora Limitless surveillées
Protection RDS	AuroraScaleout	MonitoredAcuHours	Compter (ACU-Hours)	Heures d'Aurora Scaleout ACU surveillées
Protection RDS	RDS	MonitoredVcpuHours	Compte (vCPU-Hours)	Heures de vCPU Amazon RDS surveillées

Protection Lambda	LambdaNet workLogs	AnalyzedBytes	Octets	Volume de journaux réseau Lambda analysés
Protection de l'IA	AIDataEvents	AnalyzedBytes	Octets	Volume d'événements liés aux données d'IA analysés

Dimensions des métriques

- Tous les comptes (comptes autonomes, comptes d'administrateur délégué et comptes de membres) : les mesures incluent les DataSource dimensions AccountId et.
- Comptes d'administrateurs délégués : les mesures incluent également des DataSource dimensions agrégées pour tous les comptes membres de l'organisation.

Protection contre les programmes malveillants pour S3

GuardDuty Malware Protection for S3 le plan de protection publie les mesures d'utilisation suivantes sur Amazon CloudWatch sous l'AWS/GuardDuty/MalwareProtection espace de noms :

Nom de la métrique	Unité	Description
CompletedScanCount	Nombre	Nombre d'analyses de programmes malveillants utilisant des objets S3 effectuées au cours d'une période donnée.
FailedScanCount	Nombre	Nombre d'analyses de programmes malveillants utilisant des objets S3 qui ont échoué au cours d'une période donnée.

SkippedScanCount	Nombre	Nombre d'analyses de programmes malveillants utilisant des objets S3 qui ont été ignorées au cours d'une période donnée.
InfectedScanCount	Nombre	Le nombre d'analyses d'objets malveillants S3 qui ont détecté un objet potentiellement malveillant au cours d'une période donnée.
CompletedScanBytes	Nombre	Nombre d'octets d'objets S3 scannés au cours d'une période donnée.

Dimensions des métriques

- Toutes les mesures incluent des Malware Protection Plan Id, Resource Name dimensions
- SkippedScanCount la métrique est incluse Skipped Reason comme dimension supplémentaire

Comprendre GuardDuty l'utilisation

GuardDuty Traitement des événements

Lorsque cette option est activée, consomme GuardDuty automatiquement les événements et les journaux directement à partir des sources de journal que vous avez sélectionnées Région AWS. GuardDuty ingère des événements provenant de sources de données distinctes et indépendantes afin de fournir une valeur de sécurité complète.

Important

La configuration ou les règles de filtrage de votre journal de service individuel (pour les journaux de flux VPC, les journaux DNS, les CloudTrail événements, les événements de

données S3, les journaux d'audit Kubernetes et les journaux réseau Lambda) n'ont aucune incidence sur le traitement par. logs/events GuardDuty

GuardDuty Frais de traitement des journaux de flux VPC pour les instances surveillées par GuardDuty Runtime Monitoring

Pour les instances surveillées par GuardDuty Runtime Monitoring (via l'agent EC2 Runtime ou l'agent Amazon EKS Runtime), le traitement des journaux de flux VPC ne GuardDuty sera pas facturé tant que l'agent envoie activement les données relatives aux événements [d'exécution](#). Si l'agent arrête de transmettre les données d'événements, le chargement est GuardDuty rétabli via VPC Flow Logs.

L'activation de la surveillance de l'exécution réduit l'utilisation des journaux de flux VPC dans les métriques CloudWatch d'utilisation d' GuardDuty Amazon. La désactivation de Runtime Monitoring rétablit l'utilisation des journaux de flux VPC.

Estimation des GuardDuty coûts

GuardDuty propose un essai gratuit de 30 jours par AWS compte pour la plupart des plans de protection. Pendant cette période d'essai, vous pouvez :

- Surveillez votre utilisation réelle grâce à des mesures GuardDuty d'utilisation
- Estimez vos coûts mensuels à l'aide AWS du calculateur de prix en fonction de vos habitudes d'utilisation observées

Les plans de protection suivants incluent un essai gratuit de 30 jours :

- Détection fondamentale des menaces
- Protection S3
- Protection EKS
- Surveillance d'exécution
- Protection RDS
- Protection Lambda
- Protection de l'IA
- Protection contre les programmes malveillants pour EC2 (uniquement pour les GuardDuty-initiated scans lorsqu'elle est activée avec la fonction Foundational Threat Detection)

Utilisation AWS Calculateur de prix

Vous pouvez utiliser le calculateur de [AWS prix](#) pour estimer vos GuardDuty coûts mensuels en fonction de vos habitudes d'utilisation observées. Pour créer une estimation pour GuardDuty :

1. Ouvrez le calculateur de [AWS prix](#).
2. Choisissez Create estimate (Créer une estimation).
3. Sur la page Ajouter un service, recherchez Amazon GuardDuty et choisissez Configurer.
4. Sélectionnez l' Région AWS endroit où GuardDuty est activé.
5. Dans la section Paramètres du service, entrez votre utilisation estimée pour chaque plan de protection en fonction des mesures d'utilisation observées sur Amazon CloudWatch ou sur la GuardDuty console.
6. Choisissez Ajouter à mon estimation pour afficher le coût mensuel projeté.

Note

Certaines mesures GuardDuty d'utilisation sont exprimées en octets. Lorsque vous saisissez des valeurs dans le calculateur de AWS prix, vous devrez peut-être convertir les octets dans l'unité appropriée (Mo, Go ou To). Utilisez les conversions suivantes :

- 1 Mo = 1 048 576 octets
- 1 Go = 1 073 741 824 octets
- 1 To = 1 099 511 627 776 octets

Clients de Security Hub

Security Hub propose un modèle de tarification simplifié pour GuardDuty la détection des menaces avec son plan complémentaire Threat Analytics, qui consolide la mesure de plusieurs menaces. GuardDuty DataSources Lorsque vous utilisez le plan Security Hub Threat Analytics (Security Hub avec GuardDuty) :

- Plusieurs GuardDuty DataSources sont consolidés
- Notamment, pour des raisons de simplicité, les événements Amazon EKS Audit Logs et les événements S3 Data sont convertis en Go à l'aide d'un taux de conversion fixe.

Pour créer une estimation des coûts de Security Hub, reportez-vous à [AWS la documentation de Security Hub](#).

Remarque : GuardDuty le statut de l'essai gratuit de 30 jours est indépendant de l'intégration de Security Hub. Activation ou désactivation de Security Hub :

- N'accorde pas de nouvel essai gratuit si vous avez déjà utilisé GuardDuty la période d'essai
- N'interrompt ni ne redémarre un essai gratuit en cours
- Ne prolonge pas les périodes d'essai existantes

Noms des fonctionnalités pour les plans de protection dans GuardDuty l'API

Lorsque vous activez Amazon GuardDuty pour la première fois, le traitement commence [Source de données de base](#) au sein de votre AWS environnement. GuardDuty utilise ces sources de données pour traiter un flux indépendant d'événements tels que les journaux de flux VPC, les journaux DNS et les événements AWS CloudTrail de gestion. Il analyse ensuite ces événements pour identifier les menaces de sécurité potentielles et génère des résultats dans votre compte.

Lorsqu'un ou plusieurs plans de protection sont activés, il GuardDuty utilise des données supplémentaires provenant d'autres AWS services de votre AWS environnement pour surveiller et analyser les menaces de sécurité potentielles. Ces sources de données supplémentaires sont appelées fonctionnalités.

Passer des sources de données aux fonctionnalités

Lorsque vous ajoutez des GuardDuty protections supplémentaires, telles que S3 Protection, Runtime Monitoring, Lambda Protection, etc., vous pouvez configurer la GuardDuty fonctionnalité correspondant au plan de protection. Historiquement, GuardDuty les protections étaient appelées « protections » `dataSources` dans les API. Cependant, après mars 2023, les nouveaux plans de GuardDuty protection sont désormais configurés comme tels `features` ou `nondataSources`. GuardDuty prend toujours en charge la configuration des plans de protection lancés avant mars 2023, `dataSources` par exemple via l'API, mais les nouveaux plans de protection ne sont disponibles que sous forme `features`. Pour plus d'informations sur les plans de protection concernés, consultez [GuardDuty Modifications de l'API](#).

Si vous gérez les plans de GuardDuty configuration et de protection via la console, vous n'êtes pas directement concerné par cette modification et vous n'avez aucune action à entreprendre. Cette modification affecte le comportement des API qui sont invoquées pour activer GuardDuty ou protéger les plans de protection qu'elles contiennent GuardDuty. Si vous utilisez des API ou AWS CLI pour activer ou modifier la configuration d'un plan de protection, vous devez utiliser le nom de fonctionnalité associé. Pour de plus amples informations, veuillez consulter [Mappage de `dataSources` aux `features`](#).

GuardDuty Modifications apportées à l'API en mars 2023

Les GuardDuty API configurent des fonctionnalités de protection qui ne figurent pas dans la liste des [GuardDuty sources de données de base](#). Un objet de fonctionnalité contient des détails sur les fonctionnalités, tels que le nom et l'état de la fonctionnalité, et peut contenir une configuration supplémentaire pour certains plans de protection. Cette migration affecte les API suivantes dans le Amazon GuardDuty API Reference :

- [CreateDetector](#)
- [GetDetector](#)
- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

Caractéristiques comparées aux sources de données

Historiquement, toutes les GuardDuty fonctionnalités étaient transmises via un `dataSources` objet dans l'API. À partir de mars 2023, GuardDuty préfère `features` l'objet à l'`dataSources` objet dans l'API. Toutes les sources de données antérieures possèdent des fonctionnalités correspondantes, mais il se peut que les fonctionnalités plus récentes n'en aient pas.

La liste suivante montre la comparaison entre un `dataSources` objet et un `features` objet lors d'une transmission via une API :

- L'objet `dataSources` contient des objets pour chaque type de protection et son état. L'objet `features` est une liste des fonctionnalités disponibles correspondant à chaque type de protection qu'il contient GuardDuty.

À compter de mars 2023, l'activation des fonctionnalités sera le seul moyen de configurer de nouvelles GuardDuty fonctionnalités dans votre AWS environnement.

- Le `dataSources` schéma de la demande ou de la réponse d'API est le même dans chaque Région AWS où GuardDuty est disponible. Cependant, il se peut que toutes les fonctionnalités

ne soient pas disponibles dans chaque région. Par conséquent, les noms des fonctionnalités disponibles peuvent varier en fonction de la région.

Comprendre le fonctionnement des API dotées de fonctionnalités

Les GuardDuty API continueront à renvoyer un `dataSources` objet le cas échéant, et elles renverront également un `features` objet contenant les mêmes informations dans un format différent. GuardDuty les fonctionnalités lancées avant mars 2023 seront disponibles via `dataSources` objet et `features` objet. GuardDuty les fonctionnalités lancées depuis mars 2023 ne seront disponibles que via l'`features` objet. Vous ne pouvez pas créer ou mettre à jour un détecteur, ni décrire votre AWS Organizations utilisation à la fois `dataSources` et de la notation d'`features` objets dans la même requête d'API. Pour activer les types de GuardDuty protection, vous devez migrer vos sources de données existantes vers l'`features` objet en utilisant les mêmes API qui incluent désormais également l'`features` objet.

Note

GuardDuty n'ajoutera pas de nouvelle source de données après cette modification.

GuardDuty a déconseillé l'utilisation de sources de données associées aux plans de protection. Cependant, il prend toujours en charge les [GuardDuty sources de données de base](#). Les GuardDuty meilleures pratiques recommandent d'utiliser des fonctionnalités permettant d'activer ou de modifier la configuration de n'importe quel plan de protection de votre compte.

Intégration des modifications apportées aux fonctionnalités dans les API

- Si vous gérez des GuardDuty configurations via des API, des SDK ou des CloudFormation modèles et que vous souhaitez activer de nouvelles GuardDuty fonctionnalités potentielles, vous devrez modifier votre code et votre modèle, respectivement. Pour plus d'informations, consultez les API mises à jour dans le [Amazon GuardDuty API Reference](#).
- Pour les GuardDuty fonctionnalités configurées avant cette mise à niveau, vous pouvez continuer à utiliser les API, les SDK ou le CloudFormation modèle. Toutefois, nous vous recommandons de passer à l'utilisation de l'objet `feature`.

Toutes les sources de données ont un objet de fonctionnalité équivalent. Pour de plus amples informations, veuillez consulter [Mappage de `dataSources` aux `features`](#).

- Actuellement, `additionalConfiguration` dans l'objet `features` n'est disponible que pour certains types de protection.
- Pour de tels types de protection, si votre fonctionnalité `AdditionalConfiguration` `status` est définie sur `ENABLED` mais que la configuration de votre fonctionnalité n'est pas définie sur `ENABLED`, GuardDuty aucune action n'est entreprise dans ce cas.
- Cela concerne les API suivantes :
 - [UpdateDetector](#)
 - [UpdateMemberDetectors](#)
 - [UpdateOrganizationConfiguration](#)

Mappage de **dataSources** aux **features**

Le tableau suivant montre le mappage des types de protection, `dataSources` et `features`.

GuardDuty type de protection	Nom de la source de données *	Nom de la fonctionnalité
Journaux de flux VPC	<code>flowLogs</code> (lecture seule ; modification impossible)	<code>FLOW_LOGS</code> (lecture seule ; modification impossible)
Journaux de requêtes DNS de Route53 Resolver	<code>dnsLogs</code> (lecture seule ; modification impossible)	<code>DNS_LOGS</code> (lecture seule ; modification impossible)
CloudTrail événements	<code>cloudTrail</code> (lecture seule ; modification impossible)	<code>CLOUD_TRAIL</code> (lecture seule ; modification impossible)
S3	<code>s3Logs</code>	<code>S3_DATA_EVENTS</code>
Protection EKS	<code>kubernetes.auditlogs</code>	<code>EKS_AUDIT_LOGS</code>

GuardDuty type de protection	Nom de la source de données *	Nom de la fonctionnalité
Protection contre les logiciels malveillants pour EC2	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
Événements de connexion RDS		RDS_LOGIN_EVENTS
Surveillance d'exécution EKS		EKS_RUNTIME_MONITORING
Surveillance d'exécution		RUNTIME_MONITORING
GuardDuty agent de sécurité pour les clusters Amazon EKS	GuardDuty fournit uniquement un support d'activation des fonctionnalités pour ces types de protection.	EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT

GuardDuty type de protection	Nom de la source de données *	Nom de la fonctionnalité
GuardDuty agent de sécurité pour les ECS-Fargate clusters Amazon		RUNTIME_MONITORING .additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
GuardDuty agent de sécurité pour les instances Amazon EC2		RUNTIME_MONITORING .additionalConfiguration.EC2_AGENT_MANAGEMENT
Protection Lambda		LAMBDA_NETWORK_LOGS

* GetUsageStatistics utilise ses propres noms de dataSource. Pour plus d'informations, consultez [Surveillance de GuardDuty l'utilisation et estimation des coûts](#) ou [GetUsageStatistics](#).

Sécurité sur Amazon GuardDuty

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des 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 AWS cadre des [programmes](#) de de . Pour en savoir plus sur les programmes de conformité qui s'appliquent à GuardDuty, consultez la section [AWS services concernés par programme de conformité](#) et .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation GuardDuty. Il vous explique comment procéder à la configuration GuardDuty pour atteindre 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 GuardDuty ressources.

Table des matières

- [Protection des données sur Amazon GuardDuty](#)
- [Journalisation des appels GuardDuty d'API Amazon avec AWS CloudTrail](#)
- [Identity and Access Management pour Amazon GuardDuty](#)
- [Validation de conformité pour Amazon GuardDuty](#)
- [Résilience chez Amazon GuardDuty](#)
- [Sécurité de l'infrastructure sur Amazon GuardDuty](#)
- [Amazon GuardDuty et les points de terminaison VPC d'interface \(\)AWS PrivateLink](#)

Protection des données sur Amazon GuardDuty

Le modèle de responsabilité AWS <https://aws.amazon.com/compliance/shared-responsibility-model/> s'applique à la protection des données sur Amazon GuardDuty. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble des AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité [des données et les conditions légales de la région](#) . Pour plus d'informations sur la protection des données en Europe, consultez le [Centre du règlement général sur la protection des données \(RGPD\)](#).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour enregistrer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le Guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec GuardDuty ou Services AWS utilisez

la console, l'API ou les kits de AWS développement logiciel (SDK). 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.

Chiffrement au repos

Toutes les données des GuardDuty clients sont cryptées au repos à l'aide de solutions de AWS cryptage.

GuardDuty les données, telles que les résultats, sont cryptées au repos à l'aide de AWS Key Management Service (AWS KMS) avec les clés AWS détenues.

Chiffrement en transit

GuardDuty analyse les données de journal provenant d'autres services. Il chiffre toutes les données en transit depuis ces services avec HTTPS et KMS. Une GuardDuty fois que les informations nécessaires ont été extraites des journaux, elles sont supprimées. Pour plus d'informations sur l' GuardDuty utilisation des informations provenant d'autres services, consultez la section [Sources de GuardDuty données](#).

GuardDuty les données sont cryptées lors du transit entre les services.

Refus d'utiliser vos données pour améliorer le service

Vous pouvez choisir de refuser que vos données soient utilisées pour développer GuardDuty et améliorer d'autres services de AWS sécurité en utilisant la politique de AWS Organizations désinscription. Vous pouvez choisir de vous désinscrire même si aucune donnée de ce type GuardDuty n'est actuellement collectée. Pour plus d'informations sur la procédure de désactivation, veuillez consulter [Politiques de désactivation des services IA](#) dans le Guide de l'utilisateur AWS Organizations .

Note

Pour que vous puissiez utiliser la politique de désinscription, vos AWS comptes doivent être gérés de manière centralisée par AWS Organizations. Si vous n'avez pas encore créé

d'organisation pour vos AWS comptes, consultez la section [Création et gestion d'une organisation](#) dans le Guide de AWS Organizations l'utilisateur.

Les effets de la désactivation sont les suivants :

- GuardDuty supprimera les données qu'il a collectées et stockées à des fins d'amélioration du service avant votre désinscription (le cas échéant).
- Après votre désinscription, ces données ne GuardDuty seront plus collectées ni stockées à des fins d'amélioration du service.

Les rubriques suivantes expliquent comment chaque fonctionnalité de GuardDuty ce module gère potentiellement vos données afin d'améliorer le service.

Table des matières

- [GuardDuty Surveillance du temps d'exécution](#)
- [GuardDuty Protection contre les programmes malveillants](#)

GuardDuty Surveillance du temps d'exécution

GuardDuty Runtime Monitoring permet de détecter les menaces d'exécution pour les clusters Amazon Elastic Kubernetes Service (Amazon EKS), AWS Fargate Amazon Elastic Container Service (Amazon ECS) uniquement et les instances Amazon Elastic Compute Cloud (Amazon EC2) de votre environnement. Une fois que vous avez activé Runtime Monitoring et déployé l'agent de GuardDuty sécurité pour votre ressource, vous GuardDuty commencez à surveiller et à analyser les événements d'exécution associés à votre ressource. Ces types d'événements d'exécution incluent les événements de processus, les événements de conteneur, les événements DNS, etc. Pour de plus amples informations, veuillez consulter [Types d'événements d'exécution collectés qui GuardDuty utilisent](#).

GuardDuty collecte à la fois les commandes (telles que `curlsystemctl`, `etcron`) et leurs arguments associés (tels que `start`, `stop`, `disable`) à partir de vos charges de travail. Par exemple, lorsque quelqu'un exécute `systemctl stop service-name`, GuardDuty capture à la fois la commande `systemctl` et ses arguments `stop service-name`. Ces informations détaillées permettent de GuardDuty détecter les menaces sophistiquées en analysant les modèles de commande et en corrélant plusieurs événements. Par exemple, GuardDuty peut identifier quand un attaquant tente de désactiver les services de sécurité ou exécute des fichiers malveillants connus.

Bien qu'il utilise GuardDuty activement ces données pour détecter les menaces, il n'utilise pas actuellement ces commandes et arguments à des fins d'amélioration du service (il pourrait le faire à l'avenir). Votre confiance, votre confidentialité et la sécurité de votre contenu sont nos priorités absolues et garantissent que notre utilisation est conforme à nos engagements envers vous. Pour de plus amples informations, veuillez consulter [FAQ sur la confidentialité des données](#).

GuardDuty Protection contre les programmes malveillants

GuardDuty Malware Protection analyse et détecte les programmes malveillants contenus dans les volumes EBS attachés à vos charges de travail d'instance et de conteneur Amazon EC2 potentiellement compromises, les fichiers récemment chargés dans les compartiments Amazon S3 que vous avez sélectionnés et les ressources de sauvegarde. Actuellement, GuardDuty ne collecte ni n'utilise aucun logiciel malveillant détecté pour améliorer le service. Toutefois, à l'avenir, lorsque GuardDuty Malware Protection identifiera un fichier de volume EBS, un fichier de sauvegarde ou un fichier S3 comme étant malveillant ou nuisible, GuardDuty Malware Protection collectera et stockera ce fichier pour développer et améliorer ses détections de programmes malveillants et le GuardDuty service. Ce fichier peut également être utilisé pour développer et améliorer d'autres services de sécurité AWS. Votre confiance, votre confidentialité et la sécurité de votre contenu sont nos priorités absolues et garantissent que notre utilisation est conforme à nos engagements envers vous. Pour de plus amples informations, veuillez consulter [FAQ sur la confidentialité des données](#).

Journalisation des appels GuardDuty d'API Amazon avec AWS CloudTrail

Amazon GuardDuty est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans GuardDuty. CloudTrail capture tous les appels d'API GuardDuty sous forme d'événements, y compris les appels depuis la GuardDuty console et les appels de code vers les GuardDuty API. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un bucket Amazon Simple Storage Service (Amazon S3), y compris les événements pour. GuardDuty Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite GuardDuty, 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 CloudTrail, notamment sur la manière de le configurer et de l'activer, consultez le [guide de AWS CloudTrail l'utilisateur](#).

GuardDuty informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans GuardDuty, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements AWS de service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour GuardDuty, créez un parcours. Un suivi permet CloudTrail de fournir 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 détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour en savoir plus, consultez :

- [Présentation de la création d'un journal d'activité](#)
- [Intégrations et services pris en charge par CloudTrail](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

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 :

- Si la demande a été effectuée avec des informations d'identification de connexion d'utilisateur root ou d'utilisateur IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour de plus amples informations, veuillez consulter [Élément CloudTrail userIdentity](#).

GuardDuty événements du plan de contrôle dans CloudTrail

Par défaut, CloudTrail enregistre toutes les opérations GuardDuty d'API fournies dans le [Amazon GuardDuty API Reference](#) sous forme d'événements dans CloudTrail des fichiers.

GuardDuty événements de données dans CloudTrail

[GuardDuty Surveillance du temps d'exécution](#) utilise un agent de GuardDuty sécurité déployé sur vos clusters Amazon Elastic Kubernetes Service (Amazon EKS), vos AWS Fargate instances Amazon Elastic Compute Cloud (Amazon EC2) et vos tâches (Amazon Elastic Container Service (Amazon ECS) uniquement) pour collecter un module complémentaire [Types d'événement d'exécution collectés](#) () AWS qui collecte pour vos charges de travail puis les envoie aws-guardduty-agent à des fins de détection et d'analyse des menaces. GuardDuty

Enregistrement et surveillance des événements de données

Vous pouvez éventuellement configurer les AWS CloudTrail journaux pour afficher les événements de données de votre agent GuardDuty de sécurité.

Pour créer et configurer CloudTrail, consultez la section [Événements liés aux données](#) dans le guide de l'AWS CloudTrail utilisateur et suivez les instructions relatives à la journalisation des événements de données à l'aide des sélecteurs d'événements avancés dans le Console de gestion AWS. Lorsque vous enregistrez le journal de suivi, veillez à apporter les modifications suivantes :

- Pour le type d'événement Data, choisissez GuardDutydetector.
- Pour le modèle de sélecteur de journal, choisissez Consigner tous les événements.
- Développez la vue JSON pour la configuration. Elle doit être similaire au JSON suivant :

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
```

```

    "equals": [
      "AWS::GuardDuty::Detector"
    ]
  }
]
}
]

```

Après avoir activé le sélecteur pour le parcours, accédez à la console Amazon S3 à <https://console.aws.amazon.com/s3/> l'adresse. Vous pouvez télécharger les événements de données depuis le compartiment S3 que vous avez choisi au moment de configurer les CloudTrail journaux.

Exemple : entrées de fichier GuardDuty journal

Un suivi 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 trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'événement du plan de données.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
    "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-instance/i-123412341234example",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333:aws:ec2-instance",
        "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
        "accountId": "111122223333",
        "userName": "aws:ec2-instance"
      }
    }
  },

```

```

      "attributes": {
        "creationDate": "2023-03-05T04:00:21Z",
        "mfaAuthenticated": "false"
      },
      "ec2RoleDelivery": "2.0"
    },
    "eventTime": "2023-03-05T06:03:49Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "SendSecurityTelemetry",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEEbbbbbb",
    "readOnly": false,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::GuardDuty::Detector",
      "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
    }
  }
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l>CreateIPThreatIntelSetaction (événement du plan de contrôle).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",

```

```

    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-06-14T22:54:20Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "userName": "Alice"
      }
    }
  },
  "eventTime": "2018-06-14T22:57:56Z",
  "eventSource": "guardduty.amazonaws.com",
  "eventName": "CreateThreatIntelSet",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "54.240.230.177",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
    "name": "Example",
    "format": "TXT",
    "activate": false,
    "location": "https://s3.amazonaws.com/bucket.name/file.txt"
  },
  "responseElements": {
    "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
  },
  "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
  "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "444455556666"
}

```

À partir des informations de cet événement, vous pouvez déterminer que la demande a été effectuée pour créer un Exemple de liste de menaces dans GuardDuty. Vous pouvez également voir que la demande a été effectuée par un utilisateur nommé Alice le 14 juin 2018.

Identity and Access Management pour Amazon GuardDuty

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser GuardDuty les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion de l'accès à l'aide de politiques](#)
- [Comment Amazon GuardDuty travaille avec IAM](#)
- [Identity-based exemples de politiques pour Amazon GuardDuty](#)
- [Utilisation de rôles liés aux services pour Amazon GuardDuty](#)
- [AWS politiques gérées pour Amazon GuardDuty](#)
- [Résolution des problèmes d' GuardDuty identité et d'accès à Amazon](#)

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir [Résolution des problèmes d' GuardDuty identité et d'accès à Amazon](#))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir [Comment Amazon GuardDuty travaille avec IAM](#))
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir [Identity-based exemples de politiques pour Amazon GuardDuty](#))

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. 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), d'une 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 CLI 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 par 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 Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'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'autorisation JSON que vous attachez 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 intégrées (intégrées directement dans une seule identité) 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 politique JSON que vous attachez 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 intégrées qui se trouvent 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 GuardDuty travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à GuardDuty, découvrez les fonctionnalités IAM disponibles. GuardDuty

Fonctionnalités IAM que vous pouvez utiliser avec Amazon GuardDuty

Fonctionnalité IAM	GuardDuty soutien
Identity-based politiques	Oui
Resource-based politiques	Non
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

Fonctionnalité IAM	GuardDuty soutien
Service-linked rôles	Oui

Pour obtenir une vue d'ensemble de la façon dont GuardDuty les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section [AWS Services compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

Identity-based politiques pour GuardDuty

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. 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 GuardDuty

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. [Identity-based exemples de politiques pour Amazon GuardDuty](#)

Resource-based politiques au sein de GuardDuty

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique,

cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Actions politiques pour GuardDuty

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les 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 GuardDuty actions, consultez la section [Actions définies par Amazon GuardDuty](#) dans le Service Authorization Reference.

Les actions de politique en GuardDuty cours utilisent le préfixe suivant avant l'action :

```
guardduty
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [  
  "guardduty:action1",  
  "guardduty:action2"  
]
```

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. [Identity-based exemples de politiques pour Amazon GuardDuty](#)

Ressources politiques pour GuardDuty

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*" 
```

Pour consulter la liste des types de GuardDuty ressources et leurs ARN, consultez la section [Ressources définies par Amazon GuardDuty](#) dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez [Actions définies par Amazon GuardDuty](#).

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. [Identity-based exemples de politiques pour Amazon GuardDuty](#)

Clés de conditions de politique pour GuardDuty

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les 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, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de GuardDuty condition, consultez la section [Clés de condition pour Amazon GuardDuty](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions

et ressources vous pouvez utiliser une clé de condition, consultez [Actions définies par Amazon GuardDuty](#).

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. [Identity-based exemples de politiques pour Amazon GuardDuty](#)

Listes de contrôle d'accès (ACL) dans GuardDuty

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.

Attribute-based contrôle d'accès (ABAC) avec GuardDuty

Prend en charge ABAC (identifications dans les politiques) : partiellement

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise 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 GuardDuty

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme 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 GuardDuty

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 GuardDuty

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 associées à un rôle de service peut perturber GuardDuty les fonctionnalités. Modifiez les rôles de service uniquement lorsque GuardDuty vous recevez des instructions à cet effet.

Service-linked rôles pour GuardDuty

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier 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 de détails sur la création ou la gestion des rôles GuardDuty liés à un service, consultez.

[Utilisation de rôles liés aux services pour Amazon GuardDuty](#)

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez [Services AWS qui fonctionnent avec IAM](#). Recherchez un service dans le tableau qui inclut un Yes dans la colonne des Service-linked rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Identity-based exemples de politiques pour Amazon GuardDuty

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources GuardDuty. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par GuardDuty, y compris le format des ARN pour chacun des types de ressources, consultez la section [Actions, ressources et clés de condition pour Amazon GuardDuty](#) dans le Service Authorization Reference.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de la GuardDuty console](#)
- [Autorisations requises pour activer GuardDuty](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)
- [Politique IAM personnalisée pour accorder un accès en lecture seule à GuardDuty](#)
- [Refuser l'accès aux GuardDuty résultats](#)
- [Utilisation d'une politique IAM personnalisée pour limiter l'accès aux ressources GuardDuty](#)

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer GuardDuty des ressources dans votre compte. 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 du 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 les AWS clients 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 service 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 l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS 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.

Utilisation de la GuardDuty console

Pour accéder à la GuardDuty console Amazon, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails GuardDuty des ressources 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 garantir que les utilisateurs et les rôles peuvent toujours utiliser la GuardDuty console, associez également la politique GuardDuty ConsoleAccess ou la politique ReadOnly AWS gérée aux entités. Pour plus d'informations, consultez [Ajout d'autorisations à un utilisateur](#) dans le Guide de l'utilisateur IAM.

Autorisations requises pour activer GuardDuty

Pour accorder les autorisations nécessaires aux différentes identités IAM (utilisateurs, groupes et rôles), attachez la [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) politique requise à activer GuardDuty.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'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:ListGroupsWithUser",
        "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": "*"
}
]
}

```

Politique IAM personnalisée pour accorder un accès en lecture seule à GuardDuty

Pour accorder un accès en lecture seule, GuardDuty vous pouvez utiliser la politique `AmazonGuardDutyReadOnlyAccess` gérée.

Pour créer une politique personnalisée qui accorde à un rôle, à un utilisateur ou à un groupe IAM un accès en lecture seule GuardDuty, vous pouvez utiliser l'instruction suivante :

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",

```

```

        "guardduty:GetDetector",
        "guardduty:ListFindings",
        "guardduty:GetFindings",
        "guardduty:ListIPSets",
        "guardduty:GetIPSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetInvitationsCount",
        "guardduty:GetFindingsStatistics",
        "guardduty:DescribeMalwareScans",
        "guardduty:UpdateMalwareScanSettings",
        "guardduty:GetMalwareScanSettings"
    ],
    "Resource": "*"
}
]
}

```

Refuser l'accès aux GuardDuty résultats

Vous pouvez utiliser la politique suivante pour refuser à un rôle, à un utilisateur ou à un groupe IAM l'accès aux GuardDuty résultats. Les utilisateurs ne peuvent pas consulter les résultats ni les détails les concernant, mais ils peuvent accéder à toutes les autres GuardDuty opérations :

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty>DeleteDetector",
        "guardduty:UpdateDetector",
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:CreateIPSet",
        "guardduty>DeleteIPSet",
        "guardduty:UpdateIPSet",

```

```

        "guardduty:GetIPSet",
        "guardduty:ListIPSets",
        "guardduty:CreateThreatIntelSet",
        "guardduty:DeleteThreatIntelSet",
        "guardduty:UpdateThreatIntelSet",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:ArchiveFindings",
        "guardduty:UnarchiveFindings",
        "guardduty:CreateSampleFindings",
        "guardduty:CreateMembers",
        "guardduty:InviteMembers",
        "guardduty:GetMembers",
        "guardduty:DeleteMembers",
        "guardduty:DisassociateMembers",
        "guardduty:StartMonitoringMembers",
        "guardduty:StopMonitoringMembers",
        "guardduty:ListMembers",
        "guardduty:GetMasterAccount",
        "guardduty:DisassociateFromMasterAccount",
        "guardduty:AcceptAdministratorInvitation",
        "guardduty:ListInvitations",
        "guardduty:GetInvitationsCount",
        "guardduty:DeclineInvitations",
        "guardduty:DeleteInvitations"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [

```

```
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
]
```

Utilisation d'une politique IAM personnalisée pour limiter l'accès aux ressources GuardDuty

Pour définir l'accès d'un utilisateur en GuardDuty fonction de l'ID du détecteur, vous pouvez utiliser toutes les [actions d'GuardDutyAPI](#) dans vos politiques IAM personnalisées, à l'exception des opérations suivantes :

- guardduty:CreateDetector
- guardduty:DeclineInvitations
- guardduty>DeleteInvitations
- guardduty:GetInvitationsCount
- guardduty:ListDetectors
- guardduty:ListInvitations

Utilisez les opérations suivantes dans une politique IAM pour définir l'accès d'un utilisateur en GuardDuty fonction de l'ID et de l'ID IPSet ThreatIntelSet :

- guardduty>DeleteIPSet
- guardduty>DeleteThreatIntelSet
- guardduty:GetIPSet
- guardduty:GetThreatIntelSet
- guardduty:UpdateIPSet
- guardduty:UpdateThreatIntelSet

Les exemples suivants montrent comment créer des stratégies à l'aide de certains des opérations précédentes :

- Cette politique permet à un utilisateur d'exécuter l'opération `guardduty:UpdateDetector`, à l'aide de l'ID de détecteur 1234567 dans la région us-east-1 :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
    }
  ]
}
```

- Cette politique permet à un utilisateur d'exécuter l'opération `guardduty:UpdateIPSet`, à l'aide de l'ID de détecteur 1234567 et de l'ID IPSet 000000 de la région us-east-1 :

 Note

Assurez-vous que l'utilisateur dispose des autorisations requises pour accéder aux listes d'adresses IP fiables et aux listes de menaces dans GuardDuty. Pour de plus amples informations, veuillez consulter [Configuration des prérequis pour les listes d'entités et les listes d'adresses IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],

```

```

    "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/000000"
  }
]
}

```

- Cette politique permet à un utilisateur d'exécuter l'opération `guardduty:UpdateIPSet`, à l'aide de n'importe quel ID de détecteur et de l'ID IPSet 000000 de la région us-east-1 :

Note

Assurez-vous que l'utilisateur dispose des autorisations requises pour accéder aux listes d'adresses IP fiables et aux listes de menaces dans GuardDuty. Pour de plus amples informations, veuillez consulter [Configuration des prérequis pour les listes d'entités et les listes d'adresses IP](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
    }
  ]
}

```

- Cette politique permet à un utilisateur d'exécuter l'opération `guardduty:UpdateIPSet`, à l'aide de son ID de détecteur et de n'importe quel ID IPSet de la région us-east-1 :

Note

Assurez-vous que l'utilisateur dispose des autorisations requises pour accéder aux listes d'adresses IP fiables et aux listes de menaces dans GuardDuty. Pour de plus amples

informations, veuillez consulter [Configuration des prérequis pour les listes d'entités et les listes d'adresses IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/ipset/*"
    }
  ]
}
```

L'ARN de la ressource IAM d'une GuardDuty action correspond au chemin de ressource API de cette action. La plupart des actions sont liées au détecteur ou à une sous-ressource. Par exemple `detector/detectorId`, `guardduty:GetDetector` les utilisations et les `guardduty:GetFilter utilisations` `detector/detectorId/filter/filterName`.

La plupart des résultats et des actions des membres ajoutent le nom de l'opération en tant que suffixe sur le chemin de la ressource. Les opérations de liste constituent une exception : `guardduty:ListFindings` et `guardduty:ListMembers` utilisent la base `findings` et les `member` chemins sans suffixe. Incluez le chemin complet lorsque vous définissez une politique pour les actions suivantes :

- `guardduty:GetFindings` utilise `detector/detectorId/findings/get`
- `guardduty:GetFindingsStatistics` utilise `detector/detectorId/findings/statistics`
- `guardduty:ArchiveFindings` utilise `detector/detectorId/findings/archive`
- `guardduty:GetMembers` utilise `detector/detectorId/member/get`
- `guardduty:ListFindings` utilisations `detector/detectorId/findings` (pas de suffixe)

- `guardduty:ListMembersutilisations detector/detectorId/member` (pas de suffixe)

La politique suivante octroie `guardduty:GetFindings` des autorisations pour un détecteur spécifique dans la région `us-east-1`, en utilisant le chemin complet des ressources :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:GetFindings",
    "Resource": "arn:aws:guardduty:us-east-1:111122223333:detector/a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6/findings/get"
  }]
}
```

Utilisation de rôles liés aux services pour Amazon GuardDuty

Amazon GuardDuty utilise des Gestion des identités et des accès AWS rôles liés aux [services \(IAM\)](#). Un rôle lié à un service (SLR) est un type unique de rôle IAM directement lié à GuardDuty. Service-linked les rôles sont prédéfinis par GuardDuty et incluent toutes les autorisations GuardDuty nécessaires pour appeler d'autres AWS services en votre nom.

Avec le rôle lié à un service, vous pouvez le configurer GuardDuty sans ajouter manuellement les autorisations nécessaires. GuardDuty définit les autorisations de son rôle lié à un service et, sauf si les autorisations sont définies autrement, seul GuardDuty peut assumer le rôle. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

GuardDuty prend en charge l'utilisation de rôles liés aux services dans toutes les régions où cela GuardDuty est disponible. Pour de plus amples informations, veuillez consulter [Régions et points de terminaison](#).

Vous ne pouvez supprimer le rôle GuardDuty lié à un service qu'après l'avoir désactivé pour la première fois GuardDuty dans toutes les régions où il est activé. Cela protège vos GuardDuty ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'y accéder.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez les [AWS services qui fonctionnent avec IAM](#) dans le Guide de l'utilisateur IAM et recherchez les services dont la mention Oui est indiqué dans la colonne Rôle. Service-Linked Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Service-linked autorisations de rôle pour GuardDuty

GuardDuty utilise le rôle lié aux services (SLR) nommé `AWSServiceRoleForAmazonGuardDuty`. Le rôle permet à GuardDuty d'effectuer les tâches suivantes. Il permet également à GuardDuty d'inclure les métadonnées récupérées appartenant à l'instance EC2 dans les résultats qui peuvent être générés sur la menace potentielle. Le rôle lié à un service `AWSServiceRoleForAmazonGuardDuty` fait confiance au service `guardduty.amazonaws.com` pour endosser le rôle.

Les politiques d'autorisation permettent à GuardDuty d'effectuer les tâches suivantes :

- Utilisez les actions Amazon EC2 pour gérer et récupérer des informations sur vos instances EC2, vos images et vos composants réseau tels que les VPC, les sous-réseaux et les passerelles de transit.
- Utilisez AWS Systems Manager des actions pour gérer les associations SSM sur les instances Amazon EC2 lorsque vous activez GuardDuty Runtime Monitoring avec un agent automatisé pour Amazon EC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, GuardDuty prend en compte que les instances EC2 qui ont une balise d'inclusion (`GuardDutyManaged:true`).
- Utilisez AWS Organizations des actions pour décrire les comptes associés et l'identifiant de l'organisation.
- Utilisez les actions Amazon S3 pour récupérer des informations sur les compartiments et les objets S3.
- Utilisez AWS Lambda des actions pour récupérer des informations sur vos fonctions et balises Lambda.
- Utilisez les actions Amazon EKS pour gérer et récupérer des informations sur les clusters EKS et gérer les [modules complémentaires Amazon EKS](#) sur des clusters EKS. Les actions EKS récupèrent également les informations relatives aux balises associées à GuardDuty.
- Utilisez IAM pour créer une [Service-linked autorisations de rôle pour Malware Protection for EC2](#) fois que la protection contre les programmes malveillants pour EC2 a été activée.
- Utilisez les actions Amazon ECS pour gérer et récupérer des informations sur les clusters Amazon ECS, récupérer des informations sur les tâches et les définitions de tâches, et gérer les paramètres du compte Amazon ECS avec `guarddutyActivate`. Les actions relatives à Amazon ECS permettent également d'extraire les informations relatives aux balises associées à GuardDuty.
- Utilisez les actions Amazon VPC Lattice pour activer la connectivité de l'agent Runtime Monitoring.

Le rôle est configuré avec la [stratégie gérée AWS](#) suivante, nommée `AmazonGuardDutyServiceRolePolicy`.

Pour passer en revue les autorisations relatives à cette politique, consultez [AmazonGuardDutyServiceRolePolicy](#) le AWS Managed Policy Reference Guide.

Voici la stratégie d'approbation qui est attachée au rôle lié à un service `AWSServiceRoleForAmazonGuardDuty` :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guarddduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Pour plus de détails sur les mises à jour `AmazonGuardDutyServiceRolePolicy` de la politique, consultez [GuardDuty mises à jour de AWS stratégies gérées](#). Pour recevoir des alertes automatiques concernant les modifications apportées à cette politique, abonnez-vous au fil RSS de la [Historique de la documentation](#) page.

Création d'un rôle lié à un service pour GuardDuty

Le rôle `AWSServiceRoleForAmazonGuardDuty` lié à un service est automatiquement créé lorsque vous l'activez GuardDuty pour la première fois ou lorsque vous l'activez GuardDuty dans une région prise en charge où il n'était pas activé auparavant. Vous pouvez également créer le rôle lié à un service manuellement à l'aide de la console IAM, de l'API IAM ou de l' AWS CLI API IAM.

⚠ Important

Le rôle lié au service qui est créé pour le compte d'administrateur GuardDuty délégué ne s'applique pas aux comptes des membres GuardDuty .

Vous devez configurer les autorisations de manière à permettre à un principal IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForAmazonGuardDuty` lié à un service soit créé avec succès, le principal IAM que vous utilisez GuardDuty avec doit disposer des autorisations requises. Pour accorder les autorisations requises, attachez la stratégie suivante à cet utilisateur, groupe ou rôle :

📘 Note

Remplacez l'échantillon *account ID* de l'exemple suivant par votre véritable Compte AWS identifiant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  },  
  {  
    "Effect": "Allow",  
    "Action": [  
      "iam:PutRolePolicy",  
      "iam>DeleteRolePolicy"  
    ],  
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/  
guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"  
  }  
]  
}
```

Pour de plus amples informations sur la création manuelle d'un rôle, veuillez consulter [Création d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Modifier un rôle lié à un service pour GuardDuty

GuardDuty ne vous permet pas de modifier le rôle `AWSServiceRoleForAmazonGuardDuty` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour GuardDuty

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

Important

Si vous avez activé la protection contre les programmes malveillants pour EC2, la suppression `AWSServiceRoleForAmazonGuardDuty` n'est pas automatiquement supprimée. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Si vous souhaitez supprimer `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consultez la section [Suppression d'un rôle lié à un service pour Malware Protection for EC2](#).

Vous devez d'abord désactiver GuardDuty dans toutes les régions où il est activé pour supprimer le `AWSServiceRoleForAmazonGuardDuty`. Si le GuardDuty service n'est pas désactivé lorsque vous tentez de supprimer le rôle lié au service, la suppression échoue. Pour de plus amples informations, veuillez consulter [Suspension ou désactivation GuardDuty](#).

Lorsque vous le désactivez GuardDuty, `AWSServiceRoleForAmazonGuardDuty` il n'est pas supprimé automatiquement. Si vous l'activez GuardDuty à nouveau, il recommencera à utiliser l'existant `AWSServiceRoleForAmazonGuardDuty`.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM AWS CLI, l'API IAM ou l'API IAM pour supprimer le rôle lié au `AWSServiceRoleForAmazonGuardDuty` service. Pour plus d'informations, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Pris en charge Régions AWS

Amazon GuardDuty prend en charge l'utilisation du `AWSServiceRoleForAmazonGuardDuty` rôle lié au service partout Régions AWS où il GuardDuty est disponible. Pour obtenir la liste des régions GuardDuty actuellement disponibles, consultez la section GuardDuty Points de terminaison et quotas [Amazon](#) dans le Référence générale d'Amazon Web Services.

Service-linked autorisations de rôle pour Malware Protection for EC2

Malware Protection pour EC2 utilise le rôle lié à un service (SLR) nommé.

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` Ce réflex permet à Malware Protection for EC2 d'effectuer des analyses sans agent afin de détecter les programmes malveillants sur votre compte. GuardDuty Il permet GuardDuty de créer un instantané du volume EBS dans votre compte et de partager cet instantané avec le compte de GuardDuty service. Après avoir GuardDuty évalué le snapshot, il inclut les métadonnées de charge de travail de l'instance EC2 et du conteneur récupérées dans les résultats de Malware Protection for EC2. Le rôle lié à un service `AWSServiceRoleForAmazonGuardDutyMalwareProtection` fait confiance au service `malware-protection.guardduty.amazonaws.com` pour endosser le rôle.

Les politiques d'autorisation relatives à ce rôle permettent à Malware Protection for EC2 d'effectuer les tâches suivantes :

- Utilisez les actions Amazon Elastic Compute Cloud (Amazon EC2) pour récupérer des informations sur vos instances, volumes et instantanés Amazon EC2. Malware Protection for EC2 permet également d'accéder aux métadonnées des clusters Amazon EKS et Amazon ECS.

- Créer des instantanés pour les volumes EBS dont la balise `GuardDutyExcluded` n'est pas définie sur `true`. Par défaut, les instantanés sont créés avec une balise `GuardDutyScanId`. Ne supprimez pas cette balise, sinon Malware Protection for EC2 n'aura pas accès aux instantanés.

 Important

Lorsque vous définissez `GuardDutyExcluded` ce paramètre sur `true`, le GuardDuty service ne pourra plus accéder à ces instantanés à l'avenir. Cela est dû au fait que les autres instructions de ce rôle lié à un service GuardDuty empêchent toute action sur les instantanés dont la valeur est définie sur `GuardDutyExcluded true`

- Autoriser le partage et la suppression d'instantanés uniquement si la balise `GuardDutyScanId` existe et que la balise `GuardDutyExcluded` n'est pas définie sur `true`.

 Note

N'autorise pas Malware Protection for EC2 à rendre les instantanés publics.

- Accédez aux clés gérées par le client, à l'exception de celles pour `GuardDutyExcluded` lesquelles une balise est définie `true`, `CreateGrant` à appeler pour créer et accéder à un volume EBS chiffré à partir de l'instantané chiffré qui est partagé avec le compte de GuardDuty service. Pour obtenir la liste des comptes de GuardDuty service pour chaque région, consultez [GuardDuty comptes de service par Région AWS](#).
- Accédez aux CloudWatch journaux des clients pour créer le groupe de journaux Malware Protection for EC2 et placez les journaux des événements d'analyse des programmes malveillants dans ce groupe de `/aws/guardduty/malware-scan-events` journaux.
- Autoriser le client à décider s'il souhaite conserver dans son compte les instantanés sur lesquels le logiciel malveillant a été détecté. Si l'analyse détecte un logiciel malveillant, le rôle lié au service permet d' GuardDuty ajouter deux balises aux instantanés : `et. GuardDutyFindingDetected` `GuardDutyExcluded`

 Note

La balise `GuardDutyFindingDetected` indique que les instantanés contiennent des logiciels malveillants.

- Déterminez si un volume est chiffré à l'aide d'une clé gérée EBS. GuardDuty effectue l'DescribeKeyaction pour déterminer key Id la EBS-managed clé de votre compte.
- Récupérez l'instantané des volumes EBS chiffrés à l'aide de Clé gérée par AWS, depuis votre ordinateur Compte AWS et copiez-le dans le. [GuardDuty compte de service](#) À cette fin, nous utilisons les autorisations GetSnapshotBlock etListSnapshotBlocks. GuardDuty scanne ensuite l'instantané dans le compte de service. Actuellement, la prise en charge de Malware Protection for EC2 pour l'analyse des volumes EBS chiffrés n'est Clé gérée par AWS peut-être pas disponible dans tous les. Régions AWS Pour de plus amples informations, veuillez consulter [Region-specific disponibilité des fonctionnalités](#).
- Autorisez Amazon EC2 à appeler au AWS KMS nom de Malware Protection for EC2 pour effectuer plusieurs actions cryptographiques sur les clés gérées par le client. Des actions telles que kms:ReEncryptTo et kms:ReEncryptFrom sont nécessaires pour partager les instantanés chiffrés avec les clés gérées par le client. Seules les clés suivantes pour lesquelles la balise GuardDutyExcluded n'est pas définie true sur sont accessibles.

Le rôle est configuré avec la [stratégie gérée AWS](#) suivante, nommée AmazonGuardDutyMalwareProtectionServiceRolePolicy.

Pour passer en revue les autorisations relatives à cette politique, consultez [AmazonGuardDutyMalwareProtectionServiceRolePolicy](#) le AWS Managed Policy Reference Guide.

La stratégie d'approbation suivante est attachée au rôle lié à un service AWSServiceRoleForAmazonGuardDutyMalwareProtection :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```


Création d'un rôle lié à un service pour Malware Protection for EC2

Le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié à un service est automatiquement créé lorsque vous activez la Protection contre les programmes malveillants pour EC2 pour la première fois ou que vous activez la Protection contre les programmes malveillants pour EC2 dans une région prise en charge où elle n'était pas activée auparavant. Vous pouvez également créer le rôle lié à un service `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manuellement, via la console IAM, la CLI IAM ou l'API IAM.

Note

Par défaut, si vous êtes nouveau sur Amazon GuardDuty, la protection contre les programmes malveillants pour EC2 est automatiquement activée.

Important

Le rôle lié au service qui est créé pour le compte d' GuardDuty administrateur délégué ne s'applique pas aux comptes des membres GuardDuty .

Vous devez configurer les autorisations de manière à permettre à un principal IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié à un service soit créé avec succès, l'identité IAM que vous utilisez doit disposer GuardDuty des autorisations requises. Pour accorder les autorisations requises, attachez la stratégie suivante à cet utilisateur, groupe ou rôle :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
```

```

        "Resource": "*",
        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": [
                    "malware-protection.guardduty.amazonaws.com"
                ]
            }
        },
    },
    {
        "Effect": "Allow",
        "Action": [
            "organizations:EnableAWSServiceAccess",
            "organizations:RegisterDelegatedAdministrator",
            "organizations:ListDelegatedAdministrators",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:DescribeOrganizationalUnit",
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "iam:GetRole",
        "Resource": "arn:aws:iam::*:role/*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    }
]
}

```

Pour de plus amples informations sur la création manuelle d'un rôle, veuillez consulter [Création d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Modification d'un rôle lié à un service pour Malware Protection for EC2

Malware Protection for EC2 ne vous permet pas de modifier le rôle lié au `AWSServiceRoleForAmazonGuardDutyMalwareProtection` service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Malware Protection for EC2

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

Important

Pour supprimer le `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, vous devez d'abord désactiver la protection contre les programmes malveillants pour EC2 dans toutes les régions où elle est activée.

Si la protection contre les programmes malveillants pour EC2 n'est pas désactivée lorsque vous tentez de supprimer le rôle lié à un service, la suppression échouera. Assurez-vous d'abord de désactiver la protection contre les programmes malveillants pour EC2 dans votre compte.

Lorsque vous choisissez **Désactiver** pour arrêter le service Malware Protection for EC2, celui-ci n'`AWSServiceRoleForAmazonGuardDutyMalwareProtection` est pas automatiquement supprimé. Si vous choisissez ensuite **Activer** pour redémarrer le service Malware Protection for EC2, GuardDuty vous commencerez à utiliser le service existant `AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, l'AWS interface de ligne de commande ou l'API IAM pour supprimer le rôle lié à un `AWSServiceRoleForAmazonGuardDutyMalwareProtection` service. Pour plus d'informations, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Pris en charge Régions AWS

Amazon GuardDuty prend en charge l'utilisation du `AWSServiceRoleForAmazonGuardDutyMalwareProtection` rôle lié à un service partout Régions AWS où Malware Protection for EC2 est disponible.

Pour obtenir la liste des régions GuardDuty actuellement disponibles, consultez la section GuardDuty Points de terminaison et quotas [Amazon](#) dans le Référence générale d'Amazon Web Services.

AWS politiques gérées pour Amazon GuardDuty

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de rédiger vous-même des politiques. Il faut du temps et de l'expertise pour [créer des politiques gérées par le client IAM](#) qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, consultez les politiques [AWS gérées](#) dans le Guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent 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 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'interrompent pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page [politiques gérées par AWS pour les fonctions de tâche](#) dans le Guide de l'utilisateur IAM.

L'élément de politique `Version` spécifie les règles de syntaxe de langage qui doivent être utilisées pour traiter une politique. Les politiques suivantes incluent la version actuelle prise en charge par IAM. Pour plus d'informations, consultez la section Éléments de stratégie JSON [IAM : Version](#).

AWS stratégie gérée : `AmazonGuardDutyFullAccess_v2` (recommandé)

Vous pouvez associer la politique `AmazonGuardDutyFullAccess_v2` à vos identités IAM. Cette politique permettra à un utilisateur d'avoir un accès complet pour effectuer toutes les GuardDuty actions et accéder aux ressources requises. Between `AmazonGuardDutyFullAccess_v2` et `AmazonGuardDutyFullAccess`, GuardDuty recommande la connexion `AmazonGuardDutyFullAccess_v2` car elle offre une sécurité accrue et limite les actions administratives aux responsables GuardDuty du service.

Détails de l'autorisation

La AmazonGuardDutyFullAccess_v2 politique inclut les autorisations suivantes :

- GuardDuty— Permet aux utilisateurs un accès complet à toutes les GuardDuty actions.
- IAM:
 - Permet aux utilisateurs de créer un rôle GuardDuty lié à un service.
 - Permet de consulter et de gérer les rôles IAM et leurs politiques pour GuardDuty.
 - Permet aux utilisateurs de transmettre un rôle à GuardDuty. GuardDuty utilise ce rôle pour activer la protection contre les programmes malveillants pour S3 et analyser les objets S3 pour détecter les programmes malveillants. GuardDuty utilise également ce rôle pour lancer des analyses à la recherche de Malware Protection for AWS Backup.
 - L'autorisation d'effectuer une `iam:GetRole` action
AWSServiceRoleForAmazonGuardDutyMalwareProtection détermine si le rôle lié à un service (SLR) pour Malware Protection for EC2 existe dans un compte.
- Organizations:
 - Autoriser les utilisateurs à lire (voir) la structure de GuardDuty l'organisation et les comptes.
 - Permet aux utilisateurs de désigner un administrateur délégué et de gérer les membres d'une GuardDuty organisation.

Pour passer en revue les autorisations relatives à cette politique, consultez [AmazonGuardDutyFullAccess_v2](#) dans le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AmazonGuardDutyFullAccess

Vous pouvez associer la politique AmazonGuardDutyFullAccess à vos identités IAM.

Important

Pour renforcer la sécurité et restreindre les autorisations accordées aux responsables du GuardDuty service, nous vous recommandons d'utiliser [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#).

Cette politique accorde des autorisations administratives qui permettent à un utilisateur d'accéder pleinement à toutes les GuardDuty actions et à toutes les ressources.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- **GuardDuty**— Permet aux utilisateurs un accès complet à toutes les GuardDuty actions.
- **IAM:**
 - Permet aux utilisateurs de créer le rôle GuardDuty lié au service.
 - Permet à un compte administrateur d'activer GuardDuty les comptes des membres.
 - Permet aux utilisateurs de transmettre un rôle à GuardDuty. GuardDuty utilise ce rôle pour activer la protection contre les programmes malveillants pour S3 et analyser les objets S3 pour détecter les programmes malveillants. GuardDuty utilise également ce rôle pour lancer des analyses à la recherche de Malware Protection for AWS Backup.
- **Organizations**— Permet aux utilisateurs de désigner un administrateur délégué et de gérer les membres d'une GuardDuty organisation.

L'autorisation d'effectuer une `iam:GetRole` action

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` détermine si le rôle lié à un service (SLR) pour Malware Protection for EC2 existe dans un compte.

Pour passer en revue les autorisations relatives à cette politique, consultez [AmazonGuardDutyFullAccess](#) le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AmazonGuardDutyReadOnlyAccess

Vous pouvez associer la politique AmazonGuardDutyReadOnlyAccess à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent à un utilisateur de consulter les GuardDuty résultats et les détails de votre GuardDuty organisation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- **GuardDuty**— Permet aux utilisateurs de consulter GuardDuty les résultats et d'effectuer des opérations d'API commençant par `GetList`, ou `Describe`.
- **Organizations**— Permet aux utilisateurs de récupérer des informations sur la configuration de votre GuardDuty organisation, y compris les détails du compte administrateur délégué.

Pour passer en revue les autorisations relatives à cette politique, consultez [AmazonGuardDutyReadOnlyAccess](#) le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AmazonGuardDutyServiceRolePolicy

Vous ne pouvez pas joindre de `AmazonGuardDutyServiceRolePolicy` à vos entités IAM. Cette politique AWS gérée est associée à un rôle lié à un service qui permet d' GuardDuty effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter [Service-linked autorisations de rôle pour GuardDuty](#).

GuardDuty mises à jour de AWS stratégies gérées

Consultez les détails des mises à jour apportées aux politiques AWS gérées GuardDuty depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page Historique des GuardDuty documents.

Modifier	Description	Date
AmazonGuardDutyServiceRolePolicy – Mise à jour d'une stratégie existante	Ajout des vpc-lattice:AssociateViaAWS Service autorisations vpc-lattice:CreateServiceNetworkVpcAssociation et, qui permettent d' GuardDuty utiliser les actions Amazon VPC Lattice pour activer la connectivité de l'agent Runtime Monitoring.	9 septembre 2026

Modifier	Description	Date
	<div><p>L'GdLatticeCreateManagedSvnaAssociation instruction permet GuardDuty de créer une association VPC de réseau de services pour les ressources du même compte. La GdLatticeAssociateViaAwsService déclaration permet GuardDuty de terminer l'association via Amazon VPC Lattice.</p></div> <div><pre>{ "Sid": "GdLatticeCreateManagedSvnaAssociation", "Effect": "Allow", "Action": "vpc-lattice:CreateServiceNetworkVpcAssociation", "Resource": "arn:aws:vpc-lattice:*:*:servicenetworkvpcassociation/*", "Condition": { "StringEquals": { "aws:ResourceAccou</pre></div>	

Modifier	Description	Date
	<pre>nt": "\${aws:PrincipalAccount}" } }, { "Sid": "GdLatticeAssociateViaAwsService", "Effect": "Allow", "Action": "vpc-lattice:AssociateViaAWSService", "Resource": "*" } }</pre>	
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	Ajout d'une <code>s3:ListBucket</code> autorisation pour récupérer les listes de compartiments S3 <code>ecs:DescribeTasks</code> et d' <code>ecs:DescribeTaskDefinition</code> autorisations pour récupérer des informations sur les tâches et les définitions de tâches Amazon ECS.	23 avril 2026

Modifier	Description	Date
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	<div>Ajout de l'cloudtrail:CreateServiceLinkedChannel autorisation d'activer un mécanisme supplémentaire pour la consommation d' AWS CloudTrail événements.</div> <div><pre>{ "Sid": "CloudTrailCreateServiceLinkedChannelSid", "Effect": "Allow", "Action": ["cloudtrail:CreateServiceLinkedChannel"], "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*", "Condition": { "StringEquals": { "aws:ResourceAccount": "\${aws:PrincipalAccount}" } } }</pre></div>	25 mars 2026

Modifier	Description	Date
	<pre>} } }</pre>	
AmazonGuardDutyFullAccess : obsolète	<p>Cette politique a été remplacée par une politique limitée nommée AmazonGuardDutyFullAccess_v2 .</p> <p>Après le 13 mars 2026, vous ne pourrez plus associer la AmazonGuardDutyFullAccess politique à de nouveaux utilisateurs, groupes ou rôles. Pour de plus amples informations, veuillez consulter AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 (recommandé).</p>	13 mars 2026

Modifier	Description	Date
AmazonGuardDutyFullAccess_v2 : mise à jour d'une politique existante	<div>Ajout d'une autorisation qui vous permet de transmettre un rôle IAM GuardDuty lorsque vous activez Malware Protection for AWS Backup.</div> <div><pre>{ "Sid": "AllowPassRoleToMalwareProtection", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": ["malware-protection-plan.guardduty.amazonaws.com",</pre></div>	19 novembre 2025

Modifier	Description	Date
	<pre>"malware-protectio n.guardduty.amazon aws.com"] } } }</pre>	

Modifier	Description	Date
AmazonGuardDutyFullAccess : mise à jour d'une politique existante	<div>Ajout d'une autorisation qui vous permet de transmettre un rôle IAM GuardDuty lorsque vous activez Malware Protection for AWS Backup.</div> <div><pre>{ "Sid": "AllowPassRoleToMalwareProtection", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": ["malware-protection-plan.guardduty.amazonaws.com",</pre></div>	19 novembre 2025

Modifier	Description	Date
	<pre>"malware-protection.guardduty.amazonaws.com"] } }</pre>	
AmazonGuardDutyFullAccess_v2 — Ajout d'une nouvelle politique	Ajout d'une nouvelle AmazonGuardDutyFullAccess_v2 politique. Cette option est recommandée car ses autorisations renforcent la sécurité en limitant les actions administratives aux principaux de GuardDuty service en fonction des rôles et des politiques IAM, ainsi que de l'intégration. AWS Organizations	4 juin 2025
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	L'ec2:DescribeVpcs autorisation a été ajoutée. Cela permet de suivre GuardDuty les mises à jour du VPC, par exemple en récupérant le CIDR du VPC.	22 août 2024

Modifier	Description	Date
AmazonGuardDutyFullAccess : mise à jour d'une politique existante	<div>Ajout d'une autorisation qui vous permet de transmettre un rôle IAM GuardDuty lorsque vous activez Malware Protection pour S3.</div> <div><pre>{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com" } } }</pre></div>	10 juin 2024

Modifier	Description	Date
AmazonGuardDutyServiceRolePolicy - Mettre à jour vers une politique existante.	Utilisez AWS Systems Manager des actions pour gérer les associations SSM sur les instances Amazon EC2 lorsque vous activez GuardDuty Runtime Monitoring avec un agent automatisé pour Amazon EC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les instances EC2 qui ont une balise d'inclusion (GuardDutyManaged :true).	26 mars 2024
AmazonGuardDutyServiceRolePolicy - Mettre à jour vers une politique existante.	GuardDuty a ajouté une nouvelle autorisation permettant de <code>organization:DescribeOrganization</code> récupérer l'ID d'organisation du compte Amazon VPC partagé et de définir la politique de point de terminaison Amazon VPC avec l'ID d'organisation.	9 février 2024

Modifier	Description	Date
AmazonGuardDutyMalwareProtectionServiceRolePolicy - Mettre à jour vers une politique existante.	Malware Protection for EC2 a ajouté deux autorisations : GetSnapshotBlock celle de récupérer l'instantané ListSnapshotBlocks d'un volume EBS (chiffré à l'aide de Clé gérée par AWS) depuis votre compte de service Compte AWS et de le copier sur le compte de GuardDuty service avant de lancer l'analyse des programmes malveillants.	25 janvier 2024
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	Ajout de nouvelles autorisations pour permettre d'ajouter des paramètres de compte guarddutyActivate Amazon ECS et d'effectuer des opérations de liste et de description sur les clusters Amazon ECS.	26 novembre 2023
AmazonGuardDutyReadOnlyAccess : mise à jour d'une politique existante	GuardDuty a ajouté une nouvelle politique organisations pourListAccounts .	16 novembre 2023
AmazonGuardDutyFullAccess : mise à jour d'une politique existante	GuardDuty a ajouté une nouvelle politique organisations pourListAccounts .	16 novembre 2023

Modifier	Description	Date
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	GuardDuty a ajouté de nouvelles autorisations pour prendre en charge la prochaine fonctionnalité GuardDuty EKS Runtime Monitoring.	8 mars 2023
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	<p>GuardDuty a ajouté de nouvelles autorisations pour permettre GuardDuty de créer un Service-linked rôle pour Malware Protection for EC2. Cela permettra de GuardDuty rationaliser le processus d'activation de la protection contre les programmes malveillants pour EC2.</p> <p>GuardDuty peut désormais effectuer l'action IAM suivante :</p>	21 février 2023

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
    }
  }
}
```

Modifier	Description	Date
AmazonGuardDutyFullAccess : mise à jour d'une politique existante	GuardDuty ARN mis à jour <code>iam:GetRole</code> pour <code>deux*AWSServiceRoleForAmazonGuardDutyMalwareProtection</code> .	26 juillet 2022
AmazonGuardDutyFullAccess : mise à jour d'une politique existante	<p>GuardDuty en a ajouté un nouveau <code>AWSServiceName</code> pour permettre la création d'un rôle lié à un service à l'aide <code>iam:CreateServiceLinkedRole</code> du service GuardDuty Malware Protection for EC2.</p> <p>GuardDuty peut désormais effectuer l'<code>iam:GetRole</code> action pour obtenir des informations pour <code>AWSServiceRole</code> .</p>	26 juillet 2022

Modifier	Description	Date
AmazonGuardDutyServiceRolePolicy : mise à jour d'une politique existante	<p>GuardDuty a ajouté de nouvelles autorisations pour GuardDuty permettre d'utiliser les actions réseau Amazon EC2 afin d'améliorer les résultats.</p> <p>GuardDuty peut désormais effectuer les actions EC2 suivantes pour obtenir des informations sur la façon dont vos instances EC2 communiquent. Ces informations permettent d'améliorer la précision des résultats.</p> <ul style="list-style-type: none"> • <code>ec2:DescribeVpcEndpoints</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:DescribeVpcPeeringConnections</code> • <code>ec2:DescribeTransitGatewayAttachments</code> 	3 août 2021
GuardDuty a commencé à suivre les modifications	GuardDuty a commencé à suivre les modifications apportées AWS à ses politiques gérées.	3 août 2021

Résolution des problèmes d' GuardDuty identité et d'accès à Amazon

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec GuardDuty IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans GuardDuty](#)
- [Je ne suis pas autorisé à exécuter iam :PassRole.](#)
- [Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes GuardDuty ressources.](#)

Je ne suis pas autorisé à effectuer une action dans GuardDuty

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM mateojackson tente d'utiliser la console pour afficher des informations détaillées sur une ressource *my-example-widget* fictive, mais ne dispose pas des autorisations guardduty: *GetWidget* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: guardduty:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur mateojackson doit être mise à jour pour autoriser l'accès à la ressource *my-example-widget* à l'aide de l'action guardduty: *GetWidget*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à exécuter iam :PassRole.

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter iam:PassRole l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à GuardDuty.

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 exécuter une action dans GuardDuty. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes GuardDuty ressources.

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises GuardDuty en charge, consultez [Comment Amazon GuardDuty travaille avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'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 GuardDuty

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, voir [Téléchargement de rapports dans 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 chez Amazon GuardDuty

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. 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 AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Sécurité de l'infrastructure sur Amazon GuardDuty

En tant que service géré, Amazon GuardDuty est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure

est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder GuardDuty via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Des suites de chiffrement dotées d'un secret de transmission parfait (PFS), telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Amazon GuardDuty et les points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et Amazon en GuardDuty créant un point de terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par [AWS PrivateLink](#) une technologie qui vous permet d'accéder à GuardDuty des API de manière privée sans passerelle Internet, appareil NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec GuardDuty les API. Le trafic entre votre VPC et celui qui GuardDuty ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs [interfaces réseau Elastic](#) dans vos sous-réseaux.

Pour plus d'informations, consultez la section [Interface VPC endpoints \(AWS PrivateLink\)](#) dans le Guide.AWS PrivateLink

Considérations relatives aux points de GuardDuty terminaison VPC

Avant de configurer un point de terminaison VPC d'interface pour GuardDuty, assurez-vous de consulter les [propriétés et les limites du point de terminaison d'interface](#) dans le AWS PrivateLink Guide.

GuardDuty permet d'appeler toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison VPC d'interface pour GuardDuty

Vous pouvez créer un point de terminaison VPC pour le GuardDuty service à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez [Création d'un point de terminaison d'interface](#) dans le Guide AWS PrivateLink .

Créez un point de terminaison VPC à l' GuardDuty aide du nom de service suivant :

- com.amazonaws. *region*. devoir de garde
- com.amazonaws. *region*.guardduty-fips (point de terminaison FIPS)

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API GuardDuty en utilisant son nom DNS par défaut pour la région, par exemple,guardduty.us-east-1.amazonaws.com.

Pour plus d'informations, consultez la section [Accès à un service via un point de terminaison d'interface](#) dans le AWS PrivateLink Guide.

Création d'une politique de point de terminaison VPC pour GuardDuty

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à GuardDuty. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez la section [Contrôler l'accès aux services avec des points de terminaison VPC dans le Guide](#).AWS PrivateLink

Exemple : politique de point de terminaison VPC pour les actions GuardDuty

Voici un exemple de politique de point de terminaison pour GuardDuty. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde l'accès aux GuardDuty actions répertoriées à tous les principaux sur toutes les ressources.

```
{  
  "Statement": [  

```

```
{
  "Principal": "*",
  "Effect": "Allow",
  "Action": [
    "guardduty:listDetectors",
    "guardduty:getDetector",
    "guardduty:getFindings"
  ],
  "Resource": "*"
}
```

Sous-réseaux partagés

Vous ne pouvez pas créer, décrire, modifier ou supprimer des points de terminaison d'un VPC dans des sous-réseaux qui sont partagés avec vous. Toutefois, vous pouvez utiliser les points de terminaison d'un VPC dans les sous-réseaux qui sont partagés avec vous. Pour plus d'informations sur le partage de VPC, consultez [Partager votre VPC avec d'autres comptes](#) dans le Guide de l'utilisateur Amazon VPC.

GuardDuty intégration aux services AWS de sécurité

GuardDuty peut être intégré à d'autres services AWS de sécurité. Ces services peuvent ingérer des données pour vous GuardDuty permettre de visualiser les résultats de nouvelles manières. Consultez les options d'intégration suivantes pour en savoir plus sur la façon dont ce service est configuré pour fonctionner avec GuardDuty.

Intégration GuardDuty avec AWS Security Hub CSPM

AWS Security Hub CSPM collecte des données de sécurité provenant de vos AWS comptes, de vos services et des produits partenaires tiers pris en charge afin d'évaluer l'état de sécurité de votre environnement conformément aux normes du secteur et aux meilleures pratiques. Outre l'évaluation de votre niveau de sécurité, Security Hub CSPM crée un emplacement central pour les résultats de tous vos AWS services intégrés et produits AWS partenaires. L'activation de Security Hub CSPM GuardDuty permettra automatiquement aux données de GuardDuty résultats d'être ingérées par Security Hub CSPM.

Pour plus d'informations sur l'utilisation de Security Hub CSPM avec GuardDuty , voir. [Intégration à AWS Security Hub CSPM](#)

Intégration GuardDuty à Amazon Detective

Amazon Detective utilise les données de journal de tous vos AWS comptes pour créer des visualisations de données pour vos ressources et adresses IP qui interagissent avec votre environnement. Les visualisations de Detective vous aident à enquêter rapidement et facilement sur les problèmes de sécurité. Vous pouvez passer de la GuardDuty recherche de détails à la recherche d'informations dans la console Detective une fois les deux services activés.

Pour plus d'informations sur l'utilisation de Detective avec, GuardDuty voir [Intégration à Amazon Detective](#).

Intégration à AWS Security Hub CSPM

[AWS Security Hub CSPM](#) fournit une vue complète de votre état de sécurité dans AWS et vous permet de vérifier votre environnement par rapport aux normes et aux bonnes pratiques du secteur

de la sécurité. Security Hub CSPM collecte des données de sécurité provenant de AWS comptes, de services et de produits partenaires tiers pris en charge et vous aide à analyser vos tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires.

L' GuardDuty intégration d'Amazon à Security Hub CSPM vous permet d'envoyer des résultats depuis GuardDuty Security Hub CSPM. Security Hub CSPM peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité.

Table des matières

- [Comment Amazon GuardDuty envoie ses résultats à AWS Security Hub CSPM](#)
 - [Types de résultats GuardDuty envoyés au Security Hub CSPM](#)
 - [Latence pour l'envoi de nouvelles découvertes](#)
 - [Réessayer lorsque Security Hub CSPM n'est pas disponible](#)
 - [Mise à jour des résultats existants dans Security Hub CSPM](#)
- [Afficher GuardDuty les résultats dans AWS Security Hub CSPM](#)
 - [Interprétation GuardDuty de la recherche de noms dans AWS Security Hub CSPM](#)
 - [Découverte typique de GuardDuty](#)
- [Activation et configuration de l'intégration](#)
- [Utilisation GuardDuty des contrôles dans Security Hub CSPM](#)
- [Arrêt de la publication des résultats sur Security Hub CSPM](#)

Comment Amazon GuardDuty envoie ses résultats à AWS Security Hub CSPM

Dans AWS Security Hub CSPM, les problèmes de sécurité sont suivis sous forme de découvertes. Certains résultats proviennent de problèmes détectés par d'autres AWS services ou par des partenaires tiers. Security Hub CSPM dispose également d'un ensemble de règles qu'il utilise pour détecter les problèmes de sécurité et générer des résultats.

Security Hub CSPM fournit des outils permettant de gérer les résultats provenant de toutes ces sources. Vous pouvez afficher et filtrer les listes de résultats et afficher les informations sur un résultat. Pour de plus amples informations, consultez la section [Viewing findings](#) (Affichage des résultats) dans le Guide de l'utilisateur AWS Security Hub . Vous pouvez également suivre le statut d'une analyse dans un résultat. Pour de plus amples informations, veuillez consulter [Prendre des mesure en fonction des résultats](#) dans le Guide de l'utilisateur AWS Security Hub .

Tous les résultats du Security Hub CSPM utilisent un format JSON standard appelé AWS Security Finding Format (ASFF). Le format ASFF comprend des informations sur la source du problème, les ressources affectées et le statut actuel du résultat. Consultez [AWS Security Finding Format \(ASFF\)](#) dans le Guide de l'utilisateur AWS Security Hub .

Amazon GuardDuty est l'un des AWS services qui envoie les résultats à Security Hub CSPM.

Types de résultats GuardDuty envoyés au Security Hub CSPM

Une fois que vous avez GuardDuty activé Security Hub CSPM sur le même compte au sein du même compte Région AWS, vous commencez GuardDuty à envoyer tous les résultats générés à Security Hub CSPM. Ces résultats sont envoyés au Security Hub CSPM à l'aide du format [ASFF \(AWS Security Finding Format\)](#). Dans le format ASFF, le champ Types fournit le type de résultat.

Latence pour l'envoi de nouvelles découvertes

Lors de GuardDuty la création d'un nouveau résultat, il est généralement envoyé au Security Hub CSPM dans les cinq minutes.

Réessayer lorsque Security Hub CSPM n'est pas disponible

Si Security Hub CSPM n'est pas disponible, GuardDuty réessaie d'envoyer les résultats jusqu'à ce qu'ils soient reçus.

Mise à jour des résultats existants dans Security Hub CSPM

Après avoir envoyé un résultat à Security Hub CSPM, il GuardDuty envoie des mises à jour pour refléter les observations supplémentaires concernant l'activité de recherche à Security Hub CSPM. Les nouvelles observations relatives à ces résultats sont envoyées au Security Hub CSPM en fonction des [Étape 5 — Fréquence d'exportation des résultats](#) paramètres de votre. Compte AWS

Lorsque vous archivez ou désarchivez un résultat, GuardDuty il ne l'envoie pas au Security Hub CSPM. Toute découverte désarchivée manuellement qui devient ensuite active dans n' GuardDuty est pas envoyée au Security Hub CSPM.

Afficher GuardDuty les résultats dans AWS Security Hub CSPM

Connectez-vous à la AWS Security Hub CSPM console Console de gestion AWS et ouvrez-la à l'adresse <https://console.aws.amazon.com/securityhub/>.

Vous pouvez désormais utiliser l'une des méthodes suivantes pour afficher les GuardDuty résultats dans la console Security Hub CSPM :

Option 1 : utilisation des intégrations dans Security Hub CSPM

1. Dans le volet de navigation de gauche, choisissez Intégrations.
2. Sur la page Intégrations, vérifiez le statut d'Amazon : GuardDuty.
 - Si le statut est Acceptation des résultats, choisissez Voir les résultats à côté de Accepter les résultats.
 - Si ce n'est pas le cas, pour plus d'informations sur le fonctionnement des intégrations, consultez la section [Intégrations CSPM de Security Hub dans le guide de l'utilisateur](#).AWS Security Hub

Option 2 : utilisation des résultats dans Security Hub CSPM

1. Dans le volet de navigation de gauche, sélectionnez Findings.
2. Sur la page Résultats, ajoutez le nom du produit du filtre et entrez **GuardDuty** pour afficher uniquement GuardDuty les résultats.

Interprétation GuardDuty de la recherche de noms dans AWS Security Hub CSPM

GuardDuty envoie les résultats à Security Hub CSPM en utilisant le format [ASFF \(AWS Security Finding Format\)](#). Dans le format ASFF, le champ Types fournit le type de résultat. Les types ASFF utilisent un schéma de dénomination différent de celui des GuardDuty types. Le tableau ci-dessous détaille tous les types de GuardDuty recherche avec leur équivalent ASFF tels qu'ils apparaissent dans Security Hub CSPM.

Note

Pour certains types de GuardDuty recherche, Security Hub CSPM attribue des noms de recherche ASFF différents selon que le rôle de ressource du détail de la recherche était ACTOR ou TARGET. Pour plus d'informations, consultez [Détails d'un résultat](#).

GuardDuty type de recherche	Type de résultat ASFF
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedC redentials

GuardDuty type de recherche	Type de résultat ASFF
AttackSequence:S3/CompromisedData	TTPs/AttackSequence:S3/CompromisedData
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B

GuardDuty type de recherche	Type de résultat ASFF
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.FailedLogin

GuardDuty type de recherche	Type de résultat ASFF
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CommandAndControl:Runtime/SuspiciousCommand	TTPs/Command and Control/CommandAndControl:Runtime-SuspiciousCommand
CredentialAccess:Runtime/SensitiveFileRead	TTPs/Credential Access/CredentialAccess:Runtime-SensitiveFileRead
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior

GuardDuty type de recherche	Type de résultat ASFF
DefenseEvasion:IAMUser/BedrockLoggingDisabled	TTPs/Defense Evasion/DefenseEvasion:IAMUser-BedrockLoggingDisabled
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/KernelModuleLoaded	TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded
DefenseEvasion:Runtime/SensitiveFileModified	TTPs/Defense Evasion/DefenseEvasion:Runtime-SensitiveFileModified
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand

GuardDuty type de recherche	Type de résultat ASFF
Discovery:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:Runtime/SensitiveFileRead	TTPs/Discovery/Discovery:Runtime-SensitiveFileRead
Discovery:Runtime/SuspiciousCommand	TTPs/Discovery/Discovery:Runtime-SuspiciousCommand
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior

GuardDuty type de recherche	Type de résultat ASFF
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Impact:EC2/MaliciousDomainRequest.Custom	TTPs/Impact/Impact:EC2-MaliciousDomainRequest.Custom
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller

GuardDuty type de recherche	Type de résultat ASFF
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:EC2/MaliciousFile!Snapshot	TTPs/Execution/Execution:EC2-MaliciousFile!Snapshot
Execution:EC2/MaliciousFile!AMI	TTPs/Execution/Execution:EC2-MaliciousFile!AMI
Execution:EC2/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:EC2-MaliciousFile!RecoveryPoint

GuardDuty type de recherche	Type de résultat ASFF
Execution:S3/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:S3-MaliciousFile!RecoveryPoint
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/MaliciousFileExecuted.Custom	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted.Custom
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation

GuardDuty type de recherche	Type de résultat ASFF
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impact:IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Exfiltration:Runtime/SuspiciousCommand	TTPs/Exfiltration/Exfiltration:Runtime-SuspiciousCommand
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputation
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual

GuardDuty type de recherche	Type de résultat ASFF
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistence:IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Persistence:Runtime/SuspiciousCommand	TTPs/Persistence/Persistence:Runtime-SuspiciousCommand
Persistence:Runtime/SensitiveFileModified	TTPs/Persistence/Persistence:Runtime-SensitiveFileModified

GuardDuty type de recherche	Type de résultat ASFF
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:IAMUser/ShortTermRootCredentialUsage	TTPs/Policy:IAMUser-ShortTermRootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions

GuardDuty type de recherche	Type de résultat ASFF
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/SuspiciousCommand	Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand
PrivilegeEscalation:Runtime/SensitiveFileModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-SensitiveFileModified
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort

GuardDuty type de recherche	Type de résultat ASFF
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic

GuardDuty type de recherche	Type de résultat ASFF
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS

GuardDuty type de recherche	Type de résultat ASFF
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-Drive BySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B

GuardDuty type de recherche	Type de résultat ASFF
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind

GuardDuty type de recherche	Type de résultat ASFF
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Découverte typique de GuardDuty

GuardDuty envoie les résultats au Security Hub CSPM en utilisant le format [ASFF \(AWS Security Finding Format\)](#).

Voici un exemple de résultat typique tiré de GuardDuty.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
}
```



```

    "Title": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356.",
    "Description": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
instance by guessing the SSH password.",
    "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
    "ProductFields": {
        "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
"Unknown",
        "aws/guardduty/service/archived": "false",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
"199.241.229.197",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
        "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
        "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
"46717",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
        "aws/guardduty/service/serviceName": "guardduty",
        "aws/guardduty/service/evidence": "",
        "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
"172.31.43.6",
        "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
        "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
"INBOUND",
        "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
        "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
        "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
"SSH",
        "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
        "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
        "aws/guardduty/service/additionalInfo": "",
        "aws/guardduty/service/resourceRole": "TARGET",
        "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
        "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",

```

```

    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubect1"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IPv4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}

```

Activation et configuration de l'intégration

Pour utiliser l'intégration avec AWS Security Hub CSPM, vous devez activer Security Hub CSPM. Pour plus d'informations sur l'activation de Security Hub CSPM, consultez la section [Configuration de Security Hub](#) dans le guide de l'AWS Security Hub utilisateur.

Lorsque vous activez à la fois Security Hub CSPM GuardDuty et Security Hub, l'intégration est automatiquement activée. GuardDuty commence immédiatement à envoyer les résultats à Security Hub CSPM.

Utilisation GuardDuty des contrôles dans Security Hub CSPM

AWS Security Hub CSPM utilise des contrôles de sécurité pour évaluer vos AWS ressources et vérifier votre conformité par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Vous pouvez utiliser les contrôles relatifs aux GuardDuty ressources et aux plans de protection sélectionnés. Pour plus d'informations, consultez [Amazon GuardDuty Controls](#) dans le guide de AWS Security Hub l'utilisateur.

Pour obtenir la liste de tous les contrôles relatifs AWS aux services et aux ressources, consultez [la référence aux contrôles Security Hub CSPM](#) dans le guide de l'AWS Security Hub utilisateur.

Arrêt de la publication des résultats sur Security Hub CSPM

Pour arrêter l'envoi des résultats à Security Hub CSPM, vous pouvez utiliser la console Security Hub CSPM ou l'API.

Consultez la section [Désactivation et activation du flux de résultats d'une intégration \(console\)](#) ou [Désactivation du flux de résultats d'une intégration \(API Security Hub, AWS CLI\)](#) dans le guide de l'AWS Security Hub utilisateur.

Intégration à Amazon Detective

[Amazon Detective](#) vous aide à analyser et à enquêter rapidement sur les événements de sécurité liés à un ou plusieurs AWS comptes en générant des visualisations de données représentant le comportement et l'interaction de vos ressources au fil du temps. Detective crée des visualisations des GuardDuty résultats.

Detective ingère les détails des résultats pour tous les types de résultat et donne accès aux profils des entités afin d'enquêter sur les différentes entités impliquées dans le résultat. Une entité peut être

une Compte AWS, une AWS ressource au sein d'un compte ou une adresse IP externe qui a interagi avec vos ressources. La GuardDuty console permet de basculer vers Amazon Detective à partir des entités suivantes, en fonction du type de recherche : Compte AWS rôle IAM, utilisateur ou session de rôle, agent utilisateur, utilisateur fédéré, instance Amazon EC2 ou adresse IP.

Table des matières

- [Activation de l'intégration](#)
- [Passer à Amazon Detective à partir d'une découverte GuardDuty](#)
- [Utilisation de l'intégration avec un environnement GuardDuty multi-comptes](#)

Activation de l'intégration

Pour utiliser Amazon Detective avec, GuardDuty vous devez d'abord activer Amazon Detective. Pour plus d'informations sur l'activation de Detective, consultez [Getting started with Amazon Detective](#) dans le guide de l'utilisateur Amazon Detective.

Lorsque vous activez à la fois Detective GuardDuty et Detective, l'intégration est automatiquement activée. Une fois activé, Detective ingère immédiatement les données de vos GuardDuty découvertes.

Note

GuardDuty envoie les résultats à Detective en fonction de la fréquence d'exportation des GuardDuty résultats. Par défaut, la fréquence d'exportation pour les mises à jour des résultats existants est de 6 heures. Pour que Detective reçoive les dernières mises à jour de vos résultats, il est recommandé de modifier la fréquence d'exportation à 15 minutes dans chaque région avec laquelle vous utilisez Detective GuardDuty. Pour de plus amples informations, veuillez consulter [Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour](#).

Passer à Amazon Detective à partir d'une découverte GuardDuty

1. Connectez-vous à la <https://console.aws.amazon.com/guardduty/console>.
2. Choisissez un seul résultat dans votre tableau des résultats.
3. Choisissez Enquêter avec Detective dans le volet des informations du résultat.

4. Choisissez un aspect du résultat à examiner avec Amazon Detective. Cela permet d'ouvrir la console Detective pour ce résultat ou cette entité.

Si le basculement ne se comporte pas comme prévu, veuillez consulter [Résolution des problèmes liés au pivot](#) dans le Guide de l'utilisateur Amazon Detective.

 Note

Si vous archivez une GuardDuty découverte dans la console Detective, elle est également archivée dans la GuardDuty console.

Utilisation de l'intégration avec un environnement GuardDuty multi-comptes

Si vous gérez un environnement multi-comptes dans GuardDuty, vous devez ajouter vos comptes membres à Amazon Detective pour afficher les visualisations des données Detective relatives aux résultats et aux entités de ces comptes.

Il est recommandé d'utiliser le même compte GuardDuty administrateur que le compte administrateur pour Detective. Pour plus d'informations sur l'ajout de comptes membres dans Detective, consultez [la section Gestion des comptes](#) dans le guide de l'utilisateur Amazon Detective.

 Note

Detective est un service régional, ce qui signifie que vous devez l'activer Detective et ajouter vos comptes membres dans chaque région dans laquelle vous souhaitez utiliser l'intégration.

Suspension ou désactivation GuardDuty

Vous pouvez utiliser la GuardDuty console pour suspendre ou désactiver le GuardDuty service. L'utilisation ne vous est pas facturée GuardDuty lorsque le service est suspendu.

- Tous les comptes des membres doivent être dissociés ou supprimés pour que vous puissiez les suspendre ou les désactiver GuardDuty.
- Si vous suspendez GuardDuty, il ne surveille plus la sécurité de votre AWS environnement et ne génère plus de nouvelles découvertes. Vos résultats existants restent intacts et ne sont pas affectés par la GuardDuty suspension. Vous pouvez choisir de le réactiver GuardDuty ultérieurement.
- Lorsque vous le désactivez GuardDuty dans un compte, celui-ci ne sera désactivé que pour le compte actuellement sélectionné Région AWS. Si vous souhaitez le désactiver complètement GuardDuty, vous devez le désactiver dans chaque région où il est activé.
- Si vous le désactivez GuardDuty, vos résultats existants et la GuardDuty configuration sont perdus et ne peuvent pas être restaurés. Si vous souhaitez enregistrer vos résultats existants, vous devez les exporter avant de confirmer la désactivation GuardDuty. Pour plus d'informations sur la procédure d'exportation des résultats, veuillez consulter [Exportation des résultats générés vers Amazon S3](#).
- Si vous avez activé la protection contre les programmes malveillants pour S3 pour un ou plusieurs compartiments protégés de votre compte, la suspension ou la désactivation GuardDuty n'a aucune incidence sur le statut d'un compartiment protégé dans le cadre de la protection contre les programmes malveillants pour S3. Même après la suspension ou la désactivation GuardDuty, votre compte continuera de supporter les coûts d'utilisation associés à la fonctionnalité Malware Protection for S3. Pour plus d'informations sur la désactivation de Malware Protection pour S3, consultez [Désactivation de la protection contre les programmes malveillants pour S3 pour un compartiment protégé](#).

Pour suspendre ou désactiver GuardDuty

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Dans la GuardDuty section Suspendre, choisissez Suspendre GuardDuty ou Désactiver GuardDuty, puis Confirmez votre action.

À réactiver GuardDuty après la suspension

1. Ouvrez la GuardDuty console à l'adresse <https://console.aws.amazon.com/guardduty/>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sélectionnez Re-enable GuardDuty.

Abonnement aux annonces Amazon GuardDuty SNS

Cette section fournit des informations sur l'abonnement à Amazon SNS (Simple Notification Service) GuardDuty pour les annonces visant à recevoir des notifications concernant les nouveaux types de recherche, les mises à jour des types de recherche existants et d'autres modifications de fonctionnalités. Les notifications sont proposées dans tous les formats pris en charge par Amazon SNS.

Le GuardDuty SNS envoie une annonce concernant les mises à jour du GuardDuty service AWS à n'importe quel compte abonné. Pour recevoir des notifications concernant les résultats enregistrés dans votre compte, veuillez consulter [Traitement des GuardDuty résultats avec Amazon EventBridge](#).

Note

Votre utilisateur IAM doit disposer des autorisations `sns::subscribe` pour pouvoir s'abonner à une rubrique SNS.

Vous pouvez abonner une file d'attente Amazon SQS à cette rubrique de notification, mais vous devez utiliser un ARN de rubrique se trouvant dans la même région. Pour plus d'informations, veuillez consulter [Didacticiel : Abonnement d'une file d'attente Amazon SQS à une rubrique Amazon SNS](#) dans le Guide du développeur Amazon Simple Queue Service.

Vous pouvez également utiliser une AWS Lambda fonction pour déclencher des événements lorsque des notifications sont reçues. Pour plus d'informations, veuillez consulter [Invocation des fonctions Lambda en utilisant des notifications Amazon SNS](#) dans le Guide du développeur Amazon Simple Queue Service.

Les ARN de la rubrique Amazon SNS pour chaque région sont indiqués ci-après.

Région AWS	ARN de rubrique Amazon SNS
USA Est (Virginie du Nord) – us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements

Région AWS	ARN de rubrique Amazon SNS
Est des États-Unis (Ohio) - us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
USA Ouest (Californie du Nord) - us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
USA Ouest (Oregon) - us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
Canada (Centre) - ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
Canada Ouest (Calgary) - ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
Europe (Stockholm) - eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
Europe (Irlande) - eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

Région AWS	ARN de rubrique Amazon SNS
Europe (Londres) - eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
Europe (Paris) - eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
Europe (Francfort) - eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
Europe (Zurich) - eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
Asie-Pacifique (Hong Kong) - ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
Asie-Pacifique (Tokyo) – ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
Asie-Pacifique (Séoul) - ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

Région AWS	ARN de rubrique Amazon SNS
Asie-Pacifique (Singapour) - ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
Asie-Pacifique (Sydney) - ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
Asie-Pacifique (Mumbai) - ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
Amérique du Sud (São Paulo) - sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
AWS GovCloud (US-West) - us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
Chine (Pékin) - cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
Chine (Ningxia) - cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

Région AWS	ARN de rubrique Amazon SNS
Moyen-Orient (Bahreïn) - me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
Moyen-Orient (Émirats arabes unis) - me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
Europe (Milan) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Europe (Espagne) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (US-East) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asie-Pacifique (Osaka) - ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Asie-Pacifique (Jakarta) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

Région AWS	ARN de rubrique Amazon SNS
Asie-Pacifique (Hyderabad) - ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
Asie-Pacifique (Melbourne) - ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
Asie-Pacifique (Malaisie) - ap-southeast-5	arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements
Israël (Tel Aviv) - il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements
Asie-Pacifique (Thaïlande) - ap-southeast-7	arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements
Mexique (centre) - mx-central-1	arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements
Asie-Pacifique (Taipei) - ap-east-2	arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements

Pour vous abonner à l'e-mail de notification de GuardDuty mise à jour dans le Console de gestion AWS

1. Ouvrez la console Amazon SNS à l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la liste des régions, choisissez la même région que celle dans laquelle se trouve l'ARN de la rubrique à laquelle vous souhaitez vous abonner. L'exemple utilise la région us-west-2.
3. Dans le panneau de navigation de gauche, choisissez Abonnements, puis Créer un abonnement.
4. Dans la boîte de dialogue Créer un abonnement, pour ARN de la rubrique, collez l'ARN de la rubrique : `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Pour Protocole, choisissez E-mail. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir la notification.
6. Choisissez Créer un abonnement.
7. Dans votre application de messagerie, ouvrez le message provenant AWS des notifications et ouvrez le lien pour confirmer votre abonnement.

Votre navigateur Web affiche une réponse de confirmation provenant de Amazon SNS.

Pour vous abonner à l'e-mail de notification de GuardDuty mise à jour avec AWS CLI

1. Exécutez la commande suivante avec l' AWS CLI :

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-  
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-  
endpoint your_email@your_domain.com
```

2. Dans votre application de messagerie, ouvrez le message provenant AWS des notifications et ouvrez le lien pour confirmer votre abonnement.

Votre navigateur Web affiche une réponse de confirmation provenant de Amazon SNS.

Format du message Amazon SNS

Exemple de message de notification GuardDuty général :

```
{  
  "Type" : "Notification",
```

```

    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":{\"title\":\"Updated AmazonGuardDutyFullAccess_v2 policy\",\"body\":\"Added permission that allows you to pass an IAM role to GuardDuty when you enable Malware Protection for S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-awsmanpol.html#security-iam-awsmanpol-AmaonGuardDutyFullAccess-v2\"]}}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7HpV/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrljljg==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}

```

La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :

```

{
    "version": "1",
    "type": "GENERAL",
    "message": [
        {
            "title": "Updated AmazonGuardDutyFullAccess policy",
            "body": "Added permission that allows you to pass an IAM role to
GuardDuty when you enable Malware Protection for S3.",
            "links": [
                "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmaonGuardDutyFullAccess-v2"
            ]
        }
    ]
}

```

Un exemple de message de notification de GuardDuty mise à jour concernant de nouvelles découvertes est présenté ci-dessous :

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FINDINGS\", \"findingDetails\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html\", \"findingType\":\"UnauthorizedAccess:EC2/TorClient\", \"findingDescription\":\"This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as initial gateways into a Tor network. This traffic can indicate that this EC2 instance is acting as a client on a Tor network. A common use for a Tor client is to circumvent network monitoring and filter for access to unauthorized or illicit content. Tor clients can also generate nefarious Internet traffic, including attacking SSH servers. This activity can indicate that your EC2 instance is compromised.\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :

```
{
  "version": "1",
  "type": "NEW_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "findingDescription": "This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as
```



```
initial gateways into a Tor network. This traffic can indicate that this EC2 instance
is acting as a client on a Tor network. A common use for a Tor client is to circumvent
network monitoring and filter for access to unauthorized or illicit content. Tor
clients can also generate nefarious Internet traffic, including attacking SSH servers.
This activity can indicate that your EC2 instance is compromised."
```

```
    ]]
}
```

Un exemple de message de notification de GuardDuty mise à jour concernant GuardDuty les mises à jour des fonctionnalités est illustré ci-dessous :

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails\
\": [{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\": \"https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :

```
{
  "version": "1",
  "type": "NEW_FEATURES",
  "featureDetails": [{
```

```

    "featureDescription": "Customers with high-volumes of global CloudTrail events
    should see a net positive impact on their GuardDuty costs.",
    "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
    guardduty_data-sources.html#guardduty_controlplane"
  }}
}
```

Un exemple de message de notification de GuardDuty mise à jour concernant les résultats mis à jour est illustré ci-dessous :

```

{
  "Type": "Notification",
  "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message": "{\\\"version\\\":\\\"1\\\",\\\"type\\\":\\\"UPDATED_FINDINGS\\\",
  \\\"findingDetails\\\":[{\\\"link\\\":\\\"https://docs.aws.amazon.com//guardduty/latest/ug/
  guardduty_unauthorized.html\\\",\\\"findingType\\\":\\\"UnauthorizedAccess:EC2/TorClient\\\",
  \\\"description\\\":\\\"Increased severity value from 5 to 8.\\\"}]]\",
  "Timestamp": "2018-03-09T00:25:43.483Z",
  "SignatureVersion": "1",
  "Signature": "XWox8GDGLRiCgD0Xlo/
  fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
  +4AQD/V/QjrhsEnlj+GaiW
  +ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
  YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
  +BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
  SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
  Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
  west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :

```

{
  "version": "1",
  "type": "UPDATED_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
    guardduty_unauthorized.html",
```

```
    "findingType": "UnauthorizedAccess:EC2/TorClient",  
    "description": "Increased severity value from 5 to 8."  
  }  
}
```

GuardDuty Quotas Amazon

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est Region-specific. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas pour GuardDuty, ouvrez la [console Service Quotas](#). Dans le volet de navigation, choisissez Services AWS et sélectionnez Amazon GuardDuty.

Pour demander une augmentation de quota, consultez [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas.

Vous Compte AWS disposez des quotas suivants pour Amazon GuardDuty par région.

Note

- Pour les quotas spécifiques à GuardDuty Malware Protection for EC2, consultez [Quotas dans la protection contre les programmes malveillants pour EC2](#).
- Pour les quotas spécifiques à Malware Protection for S3, consultez [Quotas de protection contre les programmes malveillants pour S3](#).

GuardDuty quotas par région

Ressource	Par défaut	Commentaires
Détecteurs	1	<p>Nombre maximal de ressources de détecteur que vous pouvez créer par compte AWS et par région.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>

Ressource	Par défaut	Commentaires
Filtres	100	<p>Le nombre maximum de filtres enregistrés par AWS compte et par région.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Recherche de la période de conservation	90 jours	<p>Nombre maximal de jours pendant lesquels une découverte est conservée.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Adresses IP et plages d'adresses CIDR par liste d'adresses IP fiables	2 000	<p>Nombre maximal d'adresses IP et de plages d'adresses CIDR que vous pouvez inclure dans une seule liste d'adresses IP fiables.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>

Ressource	Par défaut	Commentaires
Adresses IP et plages d'adresses CIDR par liste d'adresses IP de menace	250 000	<p>Le nombre maximum d'adresses IP et de plages CIDR que vous pouvez inclure dans une liste d'adresses IP de menaces.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Liste des entités par menace	1 000	<p>Le nombre maximum d'entités que vous pouvez inclure dans une seule liste d'entités de menace.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Liste des entités par entité de confiance	1 000	<p>Le nombre maximum d'entités que vous pouvez inclure dans une liste d'entités de confiance.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>

Ressource	Par défaut	Commentaires
Taille maximale du fichier	35 MO	<p>Taille de fichier maximale pour le fichier utilisé pour télécharger une liste d'entités ou une liste d'adresses IP.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Comptes membres (sur invitation) : 1 000	5000	<p>Nombre maximal de comptes membres associés à un compte administrateur.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>

Ressource	Par défaut	Commentaires
Comptes membres	50 000	<p>Nombre maximal de comptes membres associés à un compte administrateur via AWS Organizations. Cela inclut les comptes membres ajoutés à l'organisation sur invitation.</p> <p>Cette valeur par défaut dépend de votre quota actuel de comptes membres dans AWS Organizations. Le nombre de comptes membres ajoutés GuardDuty ne AWS Organizations peut pas dépasser le nombre de comptes membres de votre organisation. Pour plus d'informations sur le nombre de Comptes AWS dans une organisation, voir Valeurs maximales et minimales dans le Guide de AWS Organizations l'utilisateur.</p>

Ressource	Par défaut	Commentaires
Ensembles d'informations sur les menaces (liste d'adresses IP)	6	<p>Le nombre maximum de listes d'adresses IP de menaces que vous pouvez ajouter Compte AWS par région.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Ensembles d'adresses IP fiables (liste d'adresses IP)	1	<p>Le nombre maximum de listes d'adresses IP fiables pouvant être téléchargées et activées Compte AWS par région.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>
Listes d'entités menaçantes	6	<p>Le nombre maximum de listes d'entités menaçantes que vous pouvez ajouter Compte AWS par région.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>

Ressource	Par défaut	Commentaires
Liste des entités de confiance	1	<p>Le nombre maximum de listes d'entités de confiance pouvant être téléchargées et activées Compte AWS par région.</p> <p>Vous ne pouvez pas demander d'augmentation de quota.</p>

GuardDuty Support pour les instances gérées

Le tableau suivant indique la prise en charge des différentes fonctionnalités pour les différents types d'instances gérées. GuardDuty

Type de fonctionnalité gérée	Support de surveillance du temps d'exécution	Protection contre les logiciels malveillants pour le support EC2
Mode automatique Amazon EKS	Pris en charge	Pris en charge
Instance AWS Fargate gérée Amazon ECS	Non pris en charge	Pris en charge
Instance gérée Lambda	Non pris en charge	Non pris en charge

Résolution des problèmes liés à Amazon GuardDuty

Lorsque vous rencontrez des problèmes liés à l'exécution d'une action spécifique à GuardDuty, consultez les rubriques de cette section.

Rubriques

- [Exportation des résultats vers Amazon S3 : erreur d'accès](#)
- [Protection contre les programmes malveillants pour les problèmes liés à EC2](#)
- [Problèmes de surveillance du temps d'exécution](#)
- [Autres problèmes de résolution des problèmes](#)

Exportation des résultats vers Amazon S3 : erreur d'accès

Lorsque vous exportez des GuardDuty résultats vers un compartiment Amazon S3 (destination de publication), si vous GuardDuty ne parvenez pas à accéder à cette destination de publication, une erreur d'accès peut s'afficher.

Après avoir configuré les paramètres pour exporter les résultats, s'il n'est pas possible d'exporter les résultats, un message d'erreur s'affiche sur la page Paramètres de la GuardDuty console. Cela peut se produire lorsque vous ne pouvez plus accéder à la ressource cible. Par exemple, si votre compartiment Amazon S3 a été supprimé ou si l'autorisation d'accès au compartiment a été modifiée. Cela peut également se produire lorsque GuardDuty vous ne pouvez plus accéder à la AWS KMS clé utilisée pour chiffrer les données de votre compartiment Amazon S3. Lorsqu'il ne peut pas exporter, il envoie une notification à l'adresse e-mail associée au compte pour fournir des informations sur ce problème.

Comment résoudre l'erreur d'accès ?

Pour résoudre le problème, assurez-vous que les ressources correspondantes existent et que GuardDuty dispose des autorisations nécessaires pour accéder aux ressources nécessaires.

Pour plus d'informations, consultez [Exportation des résultats générés vers Amazon S3](#).

Que se passe-t-il si vous ne résolvez pas cette erreur ?

Si vous ne résolvez pas le problème avant la fin de la période de conservation des résultats de 90 jours GuardDuty, vos résultats ne seront pas exportés. GuardDuty désactivera la recherche des paramètres d'exportation pour ce compte dans la région spécifique.

Pour recommencer à exporter les résultats, mettez à jour les paramètres de configuration dans la région en question.

Protection contre les programmes malveillants pour les problèmes liés à EC2

Cette section répertorie les erreurs que vous pouvez rencontrer lors de la configuration ou de l'utilisation de Malware Protection for EC2.

Manquant (obligatoire) AWS Organizations autorisation de gestion lors de l'activation de l'analyse des GuardDuty-initiated programmes malveillants

Lorsque vous souhaitez gérer plusieurs comptes en utilisant AWS Organizations et que vous obtenez cette erreur `The request failed because you do not have the required AWS Organizations management account permission.`, vous n'êtes pas autorisé à activer l'analyse des GuardDuty-initiated logiciels malveillants pour plusieurs comptes de votre organisation.

Pour plus d'informations sur l'attribution d'autorisations au compte de gestion, consultez [Mise en place d'un accès fiable pour permettre l'analyse des GuardDuty-initiated logiciels malveillants](#).

Je lance une analyse des On-demand logiciels malveillants, mais cela entraîne une erreur d'autorisation requise manquante.

Si vous recevez un message d'erreur indiquant que vous ne disposez pas des autorisations requises pour lancer une analyse des On-demand programmes malveillants sur une instance Amazon EC2, vérifiez que vous avez attaché la [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) politique à votre rôle IAM.

Si vous êtes membre d'une AWS organisation et que vous recevez toujours le même message d'erreur, connectez-vous à votre compte de gestion. Pour plus d'informations, consultez [AWS Organizations SCP — Accès refusé](#).

Je reçois un message d'GetRoleerreur iam : lors de l'utilisation de Malware Protection for EC2.

Si vous recevez cette erreurUnable to get role:

AWSServiceRoleForAmazonGuardDutyMalwareProtection, cela signifie que vous n'êtes pas autorisé à activer l'analyse des GuardDuty-initiated logiciels malveillants ou à utiliser l'analyse des On-demand logiciels malveillants. Vérifiez que vous avez associé la politique [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) à votre rôle IAM.

Je suis un compte GuardDuty administrateur qui doit activer le scan des GuardDuty-initiated logiciels malveillants mais qui n'utilise pas AWS politique gérée : AmazonGuardDutyFullAccess à gérer GuardDuty.

- Configurez le rôle IAM que vous utilisez GuardDuty pour disposer des autorisations requises pour activer l'analyse des GuardDuty-initiated programmes malveillants. Pour plus d'informations sur les autorisations requises, voir [Création d'un rôle lié à un service pour Malware Protection for EC2](#).
- Attachez le [AWS stratégie gérée : AmazonGuardDutyFullAccess_v2 \(recommandé\)](#) à votre rôle IAM. Cela vous aidera à activer l'analyse des GuardDuty-initiated logiciels malveillants pour les comptes des membres.

Problèmes de surveillance du temps d'exécution

Cette section répertorie les erreurs que vous pouvez rencontrer lors de la configuration ou de l'utilisation de Runtime Monitoring.

Problèmes de couverture du temps d'exécution

Lorsque la couverture d'exécution de vos ressources protégées devient défaillante, la GuardDuty console indique le type de problème exact. Une fois que vous avez identifié le type de problème, consultez les documents suivants pour consulter les étapes de résolution des problèmes pour chaque type de ressource pris en charge :

- [Résolution des problèmes de couverture des environnements d'exécution Amazon EC2](#)
- [Résolution des problèmes de couverture du ECS-Fargate temps d'exécution d'Amazon](#)
- [Résolution des problèmes de couverture du temps d'exécution d'Amazon EKS](#)

Résolution des erreurs liées au manque de mémoire dans Runtime Monitoring (support Amazon EC2 uniquement)

Cette section décrit les étapes de dépannage lorsque vous rencontrez une erreur de mémoire insuffisante suite [Limite du processeur et de la mémoire](#) au déploiement manuel de l'agent GuardDuty de sécurité.

Si l' GuardDuty agent systemd est arrêté à cause du out-of-memory problème et que vous estimez qu'il est raisonnable de fournir plus de mémoire à l' GuardDuty agent, vous pouvez mettre à jour la limite.

1. Ouvrez avec l'autorisation root/lib/systemd/system/amazon-guardduty-agent.service.
2. Recherchez MemoryLimit et MemoryMax mettez à jour les deux valeurs.

```
MemoryLimit=256M
MemoryMax=256M
```

3. Après avoir mis à jour les valeurs, redémarrez l' GuardDuty agent à l'aide de la commande suivante :

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Exécutez la commande suivante pour afficher l'état :

```
sudo systemctl status amazon-guardduty-agent
```

La sortie attendue indiquera la nouvelle limite de mémoire :

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Mon AWS Step Functions le flux de travail échoue de façon inattendue

Si le GuardDuty conteneur a contribué à l'échec du flux de travail, consultez [Résolution des problèmes de couverture du ECS-Fargate temps d'exécution d'Amazon](#). Si le problème persiste, pour éviter l'échec du flux de travail dû au GuardDuty conteneur, effectuez l'une des étapes suivantes :

- Ajoutez le `false` tag `GuardDutyManaged` : au cluster Amazon ECS associé.
- Désactivez la configuration automatique de l'agent pour AWS Fargate (ECS uniquement) au niveau du compte. Ajoutez la balise d'inclusion `GuardDutyManaged` : `true` au cluster Amazon ECS associé que vous souhaitez continuer à surveiller avec l'agent GuardDuty automatisé.

Autres problèmes de résolution des problèmes

Si vous ne trouvez pas de scénario adapté à votre problème, veuillez consulter les options de résolution des problèmes suivantes :

- Pour les problèmes généraux liés à l'IAM lorsque vous accédez au <https://console.aws.amazon.com/guardduty/>, consultez [Résolution des problèmes d' GuardDuty identité et d'accès à Amazon](#).
- Pour les problèmes d'authentification et d'autorisation lors de l'accès AWS AWS Console Home, consultez la section [Résolution des problèmes liés à l'IAM](#).

GuardDuty Régions et points de terminaison Amazon

Pour savoir Régions AWS où Amazon GuardDuty est disponible, consultez la section [GuardDuty Points de terminaison Amazon](#) dans le Référence générale d'Amazon Web Services.

Nous vous recommandons d'activer toutes les GuardDuty options prises en charge Régions AWS. Cela permet GuardDuty de générer des informations sur des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Cela permet également GuardDuty de surveiller les AWS CloudTrail événements pour les personnes prises en charge Régions AWS, sa capacité à détecter les activités impliquant des services mondiaux étant réduite.

Region-specific disponibilité des fonctionnalités

Une liste des différences régionales pour préciser la disponibilité des GuardDuty fonctionnalités.

Champs filtrables étendus pour et CreateFilter UpdateFilter

Les [champs filtrables supplémentaires pour les](#) règles de suppression et les filtres ne sont disponibles que dans la AWS partition (aws). Dans les autres partitions, vous pouvez continuer à utiliser les champs pris en charge par la console.

ListFindings et GetFindingsStatistics APIs

Les [ListFindings](#)API [GetFindingsStatistics](#)et disposent d'un consoleOnly indicateur temporaire. Lorsque vous utilisez l'une de ces API ou les deux, l'consoleOnlyindicateur signifie que l'API peut récupérer des résultats jusqu'à une limite maximale de 1 000.

Protection contre les logiciels malveillants pour EC2

GuardDuty prend en charge la [Protection contre les logiciels malveillants pour EC2](#) fonctionnalité dans les [Zones Locales AWS Dédiées](#).

Protection RDS

La protection RDS n'est pas prise en charge dans la région Asie-Pacifique (Taipei) (ap-east-2).

La protection RDS n'est pas prise en charge dans les Zones Locales AWS dédiées.

Type de recherche IAM — [CredentialAccess:IAMUser/CompromisedCredentials](#)

Le type de CredentialAccess:IAMUser/CompromisedCredentials recherche n'est pas pris en charge dans les régions suivantes.

Région AWS	Code région
AWS GovCloud (US-West)	us-gov-west-1
AWS GovCloud (US-East)	us-gov-east-1
Chine (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

Type de recherche IAM — [DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)

Le type de DefenseEvasion:IAMUser/BedrockLoggingDisabled recherche n'est pas pris en charge dans la région Asie-Pacifique (Hong Kongap-east-1) ().

Types de détection de la protection par l'IA

Les types [Impact:IAMUser/AnomalousModelInvocation](#) de [Impact:IAMUser/CostHarvesting](#) recherche et de recherche nécessitent Amazon Bedrock ou Amazon SageMaker AI. Régions AWS Lorsque Amazon Bedrock n'est pas disponible, GuardDuty génère ces types de recherche uniquement à partir des invocations du modèle Amazon SageMaker AI. Pour les régions dans lesquelles Amazon Bedrock est disponible, consultez la section [Amazon Bedrock prise Régions AWS en charge](#) dans le guide de l'utilisateur d'Amazon Bedrock.

Le type de [Impact:IAMUser/PromptInjection.Direct](#) recherche dépend d'Amazon Bedrock Guardrails, qui n'est pas disponible dans tous les cas. Régions AWS Ce type de recherche n'est pris en charge que dans les régions où Amazon Bedrock Guardrails est disponible. Pour consulter la liste actuelle, consultez la section [Régions prises en charge pour Amazon Bedrock Guardrails](#) dans le guide de l'utilisateur d'Amazon Bedrock.

Support général de l'API

Les API suivantes figurant dans le Amazon GuardDuty API Reference peuvent présenter des différences régionales en raison de l'indisponibilité de certaines sources de données ou fonctionnalités spécifiées Régions AWS précédemment :

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)

- [GetDetector](#)
- [GetMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

Types de résultat Amazon EC2 : [DefenseEvasion:EC2/UnusualDoHActivity](#) et [DefenseEvasion:EC2/UnusualDoTActivity](#)

Le tableau suivant indique Régions AWS où GuardDuty est disponible, mais ces deux types de recherche Amazon EC2 ne sont pas encore pris en charge.

Région AWS	Code région
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Jakarta)	ap-southeast-3

AWS GovCloud (US) Régions

Pour obtenir les dernières informations, consultez [Amazon GuardDuty](#) dans le guide de AWS GovCloud (US) l'utilisateur.

Régions de Chine

Pour obtenir les dernières informations, veuillez consulter [Disponibilité des fonctionnalités et différences de mise en œuvre](#) (langue française non garantie).

GuardDuty actions et paramètres hérités

Amazon GuardDuty a déconseillé certaines actions et certains paramètres de l'API, mais les prend toujours en charge. Il est recommandé d'utiliser les nouvelles actions et les nouveaux paramètres d'API qui remplacent les options héritées. Le tableau suivant compare les actions et paramètres hérités et nouveaux.

Héritage actions/ parameters	Nouveau actions/parameters	Comparison (Comparaison)
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Avec la même implémentation dans les deux actions, GuardDuty utilise le terme Administrator inDisassociateFromAdministratorAccount.
autoEnable paramètre dans DescribeOrganizationConfiguration et UpdateOrganizationConfiguration	autoEnableOrganizationMembers	Le compte GuardDuty administrateur peut ainsi auditer et appliquer l' GuardDuty une ou l'autre des valeurs à tous les comptes membres. autoEnableOrganizationMembers À l'aide des API, la mise à jour de la configuration de tous les comptes membres peut prendre jusqu'à 24 heures. Pour plus d'informations sur les valeurs possibles du autoEnableOrganizationMembers champ, voir auto EnableOrganizationMembers
Paramètre dataSources dans les API répertoriées dans GuardDuty	features	À partir de mars 2023, vous pouvez configurer GuardDuty Protection contre les logiciels malveillants pour EC2 et utiliser les nouveaux plans de GuardDuty protection à l'aide de features. Les plans de

Héritage actions/ parameters	Nouveau actions/parameters	Comparison (Comparaison)
Modifications apportées à l'API en mars 2023.		protection lancés avant mars 2023, y compris Malware Protection for EC2, prennent toujours en charge la configuration à l'aide dataSources de. Si vous utilisez des API pour configurer un plan de protection, chaque demande d'API peut inclure dataSources ou features, mais pas les deux.

Historique du document pour Amazon GuardDuty

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version du guide de GuardDuty l'utilisateur Amazon. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Nouvelle fonctionnalité - Règles de détection personnalisées pour la surveillance du temps d'exécution	Les règles de détection personnalisées prennent GuardDuty désormais en charge la surveillance du temps d'exécution pour détecter les activités des hôtes et des conteneurs, telles que l'augmentation des privilèges, le vol d'informations d'identification, les atteintes à la défense et les fuites de conteneurs sur Amazon EKS, Amazon EC2 et Amazon ECS on Fargate. Pour plus d'informations, consultez la section Règles de détection personnalisées pour la surveillance du temps d'exécution . Ces règles génèrent également quatre nouveaux types de résultats de surveillance du temps d'exécution. Pour plus d'informations, consultez la section Recherche de types nécessitant des règles de détection personnalisées dans les types de recherche de	15 octobre 2026

GuardDuty Runtime Monitorin

g.

Type de recherche mis à jour -
UnauthorizedAccess:IAMUser/
ResourceCredentialExfiltrat
ion.InsideAWS

La ResourceCredentialExfiltrat
ion.InsideAWS découverte
existante détecte désormais
l'exfiltration des informations
d'identification Lambda en
plus d'Amazon ECS. Pour
plus d'informations, consultez
[UnauthorizedAccess:IAMUser/
ResourceCredentialExfiltrat
ion.InsideAWS](#).

28 septembre 2026

Fonctionnalité mise à jour
- Surveillance du temps
d'exécution

GuardDuty Runtime Monitorin
g publie le nouvel agent de
sécurité version 1.17.1 pour
les ressources Amazon EKS,
Amazon EC2 et Amazon
ECS.AWS Fargate Pour plus
d'informations sur la nouvelle
version de l'agent de sécurité
et une liste de ressources
supplémentaires permettant
de mettre à jour votre agent de
sécurité, consultez la section
[Versions GuardDuty publiées
de l'agent de sécurité](#).

18 septembre 2026

[Documentation mise à jour -
Plateformes compatibles avec
le Runtime Monitoring](#)

GuardDuty Runtime Monitoring a ajouté une page consolidée sur [les architectures de processeur, les systèmes d'exploitation et les versions du noyau prises en charge](#).

Les pages de prérequis pour les instances Amazon EC2 AWS Fargate (Amazon ECS uniquement) et les clusters Amazon EKS font désormais référence à cette page pour les architectures de processeur, les distributions du système d'exploitation et les versions du noyau vérifiées. Cette page inclut désormais la version 6.18 du noyau Bottlerocket.

18 septembre 2026

[Champs d' AWS CloudTrail
l'événements expurgés
documentés pour les règles de
détection personnalisées](#)

Ajout d'instructions expliquant qu'un AWS service peut supprimer la valeur d'un champ dans les AWS CloudTrail événements qu'il publie et qu'une règle de détection personnalisée dont la logique de détection dépend d'un champ expurgé ne correspond pas. Pour plus d'informations, consultez la section [Champs d'événements expurgés](#).

18 septembre 2026

[La protection par l'IA contribue à la détection des séquences d'attaques](#)

GuardDuty La détection étendue des menaces inclut désormais les résultats de la protection par l' GuardDuty IA parmi les signaux qu'elle met en corrélation pour détecter une séquence d'attaque. Pour plus d'informations, consultez la section [Détection GuardDuty étendue des menaces](#) et [protection par l'GuardDuty IA](#).

17 septembre 2026

[Rôle GuardDuty lié à un service \(SLR\) mis à jour](#)

GuardDuty a mis à jour le rôle lié au service (SLR) pour inclure les `vpc-lattice:CreateServiceNetworkVpcAssociation` autorisations et. `vpc-lattice:AssociateViaAWS` Service Ces autorisations permettent d' GuardDuty utiliser les actions Amazon VPC Lattice pour activer la connectivité de l'agent Runtime Monitoring. Pour plus d'informations, consultez la section [Autorisations de Service-linked rôle pour GuardDuty](#).

9 septembre 2026

[Nouvelle fonctionnalité -
Règles de détection personnalisées](#)

GuardDuty introduit les règles de détection personnalisées, une bibliothèque organisée de règles de détection alignées sur les techniques des auteurs de menaces. Vous pouvez parcourir, activer et gérer les règles afin de détecter des techniques spécifiques dans votre environnement. Pour plus d'informations, consultez la section [Règles de détection personnalisées](#).

1 septembre 2026

[Fonctionnalité mise à jour
— GuardDuty Investigation
\(version préliminaire\)](#)

Suppression de la limite de 100 comptes pour les enquêtes au niveau de l'organisation. Les enquêtes sur les organisations analysent désormais tous les comptes de votre organisation. Pour plus d'informations, consultez la section [GuardDutyInvestigation](#).

24 août 2026

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la nouvelle version 1.16.0 de l'agent de sécurité pour les ressources Amazon EKS, Amazon EC2 et Amazon ECS.AWS Fargate Pour plus d'informations sur la nouvelle version de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité.](#)

17 juillet 2026

[Nouveau type de recherche - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS](#) et type de recherche mis à jour - [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)

GuardDuty introduit un nouveau type de recherche qui détecte lorsque les AWS informations d'identification temporaires créées pour une tâche Amazon ECS sont utilisées à partir d'une autre tâche Compte AWS. En outre, le ResourceCredentialExfiltration.OutsideAWS résultat existant détecte désormais l'exfiltration des informations d'identification des tâches Amazon ECS en plus de Lambda. Pour plus d'informations, consultez [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS](#) et [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#).

15 juillet 2026

[Nouveau plan de protection - GuardDuty AI Protection](#)

GuardDuty AI Protection détecte les menaces qui pèsent sur les charges de travail basées sur l'IA qui utilisent Amazon Bedrock et Amazon SageMaker AI. Lorsque vous activez AI Protection, vous GuardDuty analysez les événements liés aux AWS CloudTrail données provenant de ces services afin de détecter les invocations de modèles anormales, les attaques liées à la collecte des coûts et les tentatives d'injection directe et rapide. Pour plus d'informations, consultez la section [Protection de l'GuardDuty IA](#).

13 juillet 2026

[Informations supplémentaires sur les menaces dans le schéma EventBridge d'événement Amazon pour Malware Protection for S3](#)

L' EventBridge événement Amazon relatif à la protection contre les programmes malveillants pour le scan des objets S3 fournit désormais des informations supplémentaires sur les menaces. Les nouveaux champs incluent `sourceItemDetails`, `hash`, et `itemPath`. Pour plus d'informations, consultez la section [Résultat de l'analyse des objets S3](#).

7 juillet 2026

[GuardDuty Enquête \(aperçu\)](#)

Amazon propose GuardDuty désormais des AI-powere d enquêtes en avant-pre mière publique. Vous pouvez créer des enquêtes pour analyser automatiquement les GuardDuty résultats et les comptes et recevoir un résumé structuré en quelques minutes avec un score de confiance , une classification technique MITRE ATT&CK® et des recommandations exploitab les. Vous pouvez lancer des investigations à partir de la GuardDuty console, de la CLI, de l'API ou du serveur AWS MCP. La version prélimina ire est disponible dans 10 pays Régions AWS : USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), Canada (Centre), Europe (Francfort), Europe (Irlande) , Europe (Londres), Europe (Paris), Europe (Stockholm) et Asie-Pacifique (Tokyo). Pour plus d'informations, consultez la section [GuardDutyInvestiga tion](#).

22 juin 2026

[Amazon RDS pour MariaDB et MySQL](#)

Database Insights est désormais disponible.

11 juin 2026

[Fonctionnalité mise à jour - Protection contre les logiciels malveillants pour S3](#)

GuardDuty a augmenté les quotas de protection contre les programmes malveillants pour S3 en ce qui concerne le nombre maximum de fichiers pouvant être extraits et analysés à partir d'une archive, ainsi que les niveaux maximaux d'archives imbriquées pouvant être extraites. Pour plus d'informations, consultez la section [Quotas dans Malware Protection for S3](#).

9 juin 2026

[Nouveaux types de recherche pour la surveillance du temps d'exécution - Sensitive FileModified](#)

GuardDuty Runtime Monitoring introduit 3 nouveaux types de détection qui vous informent lorsqu'un fichier système sensible à la sécurité d'une instance ou d'un conteneur Amazon EC2 a été modifié, ce qui peut permettre à un adversaire de persister, d'augmenter ses privilèges ou d'échapper à la détection. Pour plus d'informations, consultez [Persistence:Runtime/SensitiveFileModified](#), [PrivilegeEscalation:Runtime/SensitiveFileModified](#) et [DefenseEvasion:Runtime/SensitiveFileModified](#).

2 juin 2026

Fonctionnalité mise à jour - Recherche de critères de filtre	Les champs non pris en charge ont été supprimés de la liste des critères de recherche . Pour plus d'informations, voir Filtrer les résultats dans GuardDuty .	29 mai 2026
Deux types de trouvailles retirés	Les types PrivilegeEscalation:Kubernetes/PrivilegedContainer et Persistence:Kubernetes/ContainerWithSensitiveMount finding ont été retirés.	29 mai 2026
Fonctionnalité mise à jour - Surveillance du temps d'exécution	GuardDuty Surveillance du temps d'exécution Ajout du support pour la version 1.36 de Kubernetes. Pour plus d'informations, consultez la section Conditions préalables à la surveillance du temps d'exécution .	28 mai 2026
Fonctionnalité mise à jour - Surveillance du temps d'exécution	GuardDuty Runtime Monitoring publie la nouvelle version 1.15.0 de l'agent de sécurité pour les ressources Amazon ECS.AWS Fargate Pour plus d'informations sur la nouvelle version de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section Versions GuardDuty publiées de l'agent de sécurité .	28 mai 2026

[Fonctionnalité mise à jour](#)
[- Détection étendue des menaces](#)

GuardDuty Extended Threat Detection ajoute cinq nouveaux types d'indicateurs aux détails de la séquence d'attaque : MALICIOUS_PACKAGE, MISCONFIGURATION, REACHABILITY, SENSITIVE_DATA et VULNERABILITY. Pour plus d'informations, consultez la section [Détails de la recherche de séquences d'attaques](#).

20 mai 2026

[Fonctionnalité mise à jour](#)
[- Surveillance du temps d'exécution](#)

GuardDuty Runtime Monitoring publie la nouvelle version 1.15.0 de l'agent de sécurité pour les ressources Amazon EKS et Amazon EC2. Pour plus d'informations sur la nouvelle version de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

14 mai 2026

[Mis à jour AmazonGuardDutyServiceRolePolicy](#)

Ajouté `s3:ListBucket`, `ecs:DescribeTasks`, et `ecs:DescribeTaskDefinition` autorisations pour le rôle GuardDuty lié au service. Pour plus d'informations, voir les [GuardDuty mises à jour des politiques AWS gérées](#).

23 avril 2026

[Fonctionnalité mise à jour - Surveillance du temps d'exécution](#)

GuardDuty Runtime Monitoring publie la nouvelle version 1.12.2 de l'agent de sécurité pour les ressources Amazon EKS. Pour plus d'informations sur la nouvelle version de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

22 avril 2026

[Fonctionnalité mise à jour - Champs filtrables étendus](#)

GuardDuty prend désormais en charge le filtrage sur n'importe quel champ de recherche lors de la création ou de la mise à jour des règles de suppression. Les champs d'horodatage acceptent des valeurs au format Unix Epoch en millisecondes. Pour plus d'informations, voir [Filtrer les résultats dans GuardDuty](#).

20 avril 2026

[Fonctionnalité mise à jour -
Protection contre les logiciels
malveillants pour S3](#)

La EventBridge notification des résultats de l'analyse des objets S3 inclut désormais un `statusReasons` champ `scanResultDetails` lorsqu'une analyse est ignorée. Ce champ indique la raison précise pour laquelle le scan a été ignoré. Pour plus d'informations, consultez la section État [potentiel d'analyse de l'objet S3 et état des résultats](#).

10 avril 2026

[Fonctionnalité mise à jour
- Surveillance du temps
d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.9.2 du nouvel agent de sécurité pour les ressources Amazon EC2. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

3 avril 2026

[Mis à jour AmazonGuardDutyServiceRolePolicy](#)

Ajout de l'cloudtrail:CreateServiceLinkedChannel autorisation permettant d'activer un mécanisme supplémentaire pour la consommation d' AWS CloudTrail événements. Pour plus d'informations, voir les [GuardDuty mises à jour des politiques AWS gérées](#).

25 mars 2026

[Fonctionnalité mise à jour - Surveillance du temps d'exécution](#)

GuardDuty Surveillance du temps d'exécution Ajout du support pour la version 1.35 de Kubernetes. Pour plus d'informations, consultez la section [Conditions préalables à la surveillance du temps d'exécution](#).

20 mars 2026

[La nouvelle stratégie d'accès AmazonGuardDutyFullAccess_v2 délimitée remplace AmazonGuardDutyFullAccess](#)

À compter du 13 mars 2026, la politique GuardDuty est devenue obsolète et remplacée par une AmazonGuardDutyFullAccess_v2 politique délimitée nommée. AmazonGuardDutyFullAccess_v2 Pour plus d'informations, consultez la section [politique AWS gérée : AmazonGuardDutyFullAccess_v2](#).

13 mars 2026

[Nouveau type de recherche -
CredentialAccess:IAMUser/CompromisedCredentials](#)

GuardDuty Introduit un nouveau type de recherche qui détecte lorsqu'une clé d'accès IAM potentiellement compromise est utilisée pour appeler des opérations d'API dans AWS. Pour plus d'informations, consultez [CredentialAccess:IAMUser/CompromisedCredentials](#).

6 mars 2026

[Nouveau type de recherche -
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)

GuardDuty introduit un nouveau type de recherche qui détecte lorsqu'un hôte extérieur AWS tente d'exécuter des opérations d' AWS API à l'aide AWS d'informations d'identification temporaires créées sur une AWS Lambda ressource de votre AWS environnement. Pour plus d'informations, consultez [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#).

16 décembre 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.9.1 du nouvel agent de sécurité pour les ressources Amazon EC2. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité.](#)

2 décembre 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la nouvelle version 1.12.1 de l'agent de sécurité pour les ressources Amazon EKS. Pour plus d'informations sur la nouvelle version de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité.](#)

2 décembre 2025

Fonctionnalité mise à jour - Détection étendue des menaces

GuardDuty Extended Threat Detection introduit deux nouveaux types de détection de séquences d'attaques : [AttackSequence:ECS/CompromisedCluster](#), qui aident à détecter les attaques en plusieurs étapes impliquant des instances Amazon EC2 et des clusters Amazon ECS compromis. [AttackSequence:EC2/CompromisedInstanceGroup](#) Activez la surveillance du temps d'exécution pour [optimiser la détection des menaces](#). Pour plus d'informations, consultez la section [Types de recherche de séquences d'attaques](#).

2 décembre 2025

Nouvelle fonctionnalité : les caractères génériques dans les règles de suppression

GuardDuty a amélioré ses capacités de suppression avec l'introduction de matches et de NotMatches conditions qui prennent en charge les caractères génériques. Les clients peuvent désormais utiliser * (pour correspondre à n'importe quel nombre de caractères) et ? (pour correspondre à au plus 1 caractère) sous forme de jokers lors de la création de règles de suppression. [Règles de suppression](#).

2 décembre 2025

[Nouvelle fonctionnalité -
Amazon CloudWatch Usage
Metrics Support](#)

GuardDuty introduit la publication de statistiques d'utilisation dans Amazon CloudWatch pour tous les plans de protection, permettant aux clients de surveiller l'utilisation. Pour plus d'informations, voir [Surveillance de GuardDuty l'utilisation et estimation des coûts](#)

25 novembre 2025

[Nouveau type de recherche
- DefenseEvasion:IAMUser/
BedrockLoggingDisabled](#)

GuardDuty introduit un nouveau type de recherche qui détecte lorsque la journalisation des appels du modèle Amazon Bedrock est désactivée, ce qui peut indiquer une tentative d'échapper à la détection de l'activité de la charge de travail de l'IA. Pour plus d'informations, consultez [DefenseEvasion:IAMUser/BedrockLoggingDisabled](#).

21 novembre 2025

[Nouvelle fonctionnalité -
Protection contre les logiciels
malveillants pour Backup](#)

GuardDuty Malware Protection for Backup est désormais disponible dans toutes les régions commerciales où GuardDuty elle est disponible. Cette fonctionnalité vous permet de détecter la présence potentielle de logiciels malveillants dans vos ressources de sauvegarde grâce à des analyses complètes et incrémentielles des instantanés Amazon EBS, des AMI EC2 et des points de restauration. Pour plus d'informations sur cette fonctionnalité, voir [Malware Protection for Backup](#)

19 novembre 2025

[Remplacer par AmazonGuardDutyFullAccess et
AmazonGuardDutyFullAccess_V2](#)

Autorisation ajoutée qui vous permet de transmettre un rôle IAM GuardDuty lorsque vous activez Malware Protection for Backup.

19 novembre 2025

[Nouvelle fonctionnalité :
protection contre les
programmes malveillants pour
l'analyse à la demande de S3.](#)

GuardDuty annonce Scan on Demand for Malware Protection pour S3. Grâce à cette fonctionnalité, vous pouvez utiliser la nouvelle SendObjectMalwareScan API pour déclencher des scans sur tous les objets déjà existants stockés dans vos compartiments S3. Pour plus d'informations, consultez [la section Analyse des programmes malveillants S3 à la demande.](#)

17 novembre 2025

[Fonctionnalité mise à jour
- Surveillance du temps
d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.9.0 du nouvel agent de sécurité pour les AWS Fargate ressources Amazon ECS. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez [GuardDuty la section Versions publiées de l'agent de sécurité.](#)

28 octobre 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.9.0 du nouvel agent de sécurité pour les ressources Amazon EC2. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez [GuardDuty la section Versions publiées de l'agent de sécurité](#).

23 octobre 2025

[Nouveau type de recherche](#)
[pour la surveillance du temps](#)
[d'exécution - DefenseEva](#)
[sion:Runtime/KernelModuleL](#)
[oaded](#)

GuardDuty La surveillance du temps d'exécution introduit un nouveau type de détection qui vous aide à identifier les techniques de contournement de la défense dans lesquelles les acteurs malveillants utilisent des modules du noyau pour contourner les contrôles de sécurité, modifier le fonctionnement du système et obtenir un accès permanent au système. Pour plus d'informations, consultez [DefenseEvasion:Runtime/KernelModuleLoaded](#).

15 octobre 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

Ajout de la prise en charge de la version 1.34 de Kubernetes pour les distributions du système d'exploitation et de la version de l'agent de sécurité pour les ressources Role GuardDuty SageMaker Manager pour Amazon EKS. Pour plus d'informations, consultez la section [Valider les exigences architecturales pour Amazon EKS.](#)

3 octobre 2025

[Ajout de conseils de](#)
[dépannage pour les](#)
[problèmes liés à la base de](#)
[données Amazon RDS](#)

Ajout de conseils pour résoudre les problèmes liés aux bases de données RDS susceptibles d'avoir une incidence sur les capacités de surveillance de GuardDuty RDS Protection, notamment en ce qui concerne le storage-full statut et les exigences relatives aux répliques de lecture de RDS pour PostgreSQL. Pour plus d'informations, voir [Résolution des problèmes de surveillance de la protection RDS.](#)

15 septembre 2025

[Fonctionnalité mise à jour - Surveillance du temps d'exécution](#)

Ajout de la distribution Ubuntu Noble OS avec prise en charge des versions du noyau 6.13 et 6.14 pour la surveillance du temps GuardDuty d'exécution pour Amazon EC2. Pour plus d'informations sur la version de l'agent EC2 prise en charge pour cette distribution du système d'exploitation, consultez la section [Valider les exigences architecturales pour Amazon](#) EC2.

13 septembre 2025

[Fonctionnalité mise à jour - Protection RDS](#)

Ajout du support de PostgreSQL 17 pour RDS pour les bases de données PostgreSQL surveillées par RDS Protection. GuardDuty Pour plus d'informations, voir [Bases de données prises en charge](#) dans RDS Protection.

13 septembre 2025

[Fonctionnalité mise à jour - Protection contre les logiciels malveillants pour S3](#)

GuardDuty Malware Protection for S3 augmente le quota par défaut des fichiers d'archive extraits de 1 000 à 10 000 fichiers. Pour plus d'informations, consultez la section [Quotas dans Malware Protection for S3](#).

3 septembre 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la nouvelle version 1.11 de l'agent de sécurité pour les ressources Amazon EKS. Pour plus d'informations sur la nouvelle version de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

29 août 2025

[Fonctionnalité mise à jour -](#)
[Utilisation de listes](#)

GuardDuty introduit des listes personnalisées d'entités fiables et menacées qui prennent en charge à la fois les adresses IP et les noms de domaine. GuardDuty continue de prendre en charge la liste d'adresses IP et recommande d'utiliser la liste d'entités pour une détection personnalisée des menaces. Pour plus d'informations, voir [Personnalisation de la détection des menaces à l'aide de listes d'entités et de listes d'adresses IP](#).

15 août 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la nouvelle version 1.8.0 de l'agent de sécurité pour les ressources Amazon EC2 et Amazon ECS AWS Fargate . Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité.](#)

12 août 2025

[Support pour la région Asie-Pacifique \(Taipei\)](#)

Amazon GuardDuty est désormais disponible dans la région Asie-Pacifique (Taipei) (ap-east-2). Pour l'activer GuardDuty dans cette région, consultez la section [Mise en route.](#) Vous pouvez recevoir des notifications concernant les mises à jour des GuardDuty fonctionnalités et les détections de menaces en [vous abonnent aux annonces Amazon GuardDuty SNS](#) dans cette région.

31 juillet 2025

[Fonctionnalité mise à jour -
Protection contre les logiciels
malveillants pour S3](#)

Malware Protection for S3 prend désormais en charge l'analyse d'objets d'une capacité maximale de 100 Go, contre 5 Go au lieu de 5 Go. Cela inclut à la fois les objets individuels et les fichiers d'archive extraits. Pour plus d'informations, consultez la section [Protection contre les programmes malveillants pour les quotas S3](#).

23 juillet 2025

[Fonctionnalité mise à jour -
Ajout du propriétaire attendu
du bucket dans les listes
d'adresses IP de confiance et
de menaces](#)

GuardDuty a ajouté le champ Propriétaire du compartiment attendu pour les listes d'adresses IP fiables et de menaces. Dans ce champ facultatif, vous pouvez spécifier un Compte AWS identifiant qui GuardDuty sera utilisé pour vérifier la propriété du compartiment Amazon S3. Pour obtenir des informations supplémentaires, consultez la section [Utilisation de listes d'adresses IP approuvées et de listes de menaces](#).

16 juillet 2025

Fonctionnalité mise à jour - Détection étendue des menaces

GuardDuty Extended Threat Detection étend désormais la prise en charge des clusters Amazon EKS en corrélant plusieurs signaux de sécurité entre les journaux d'audit EKS, le comportement d'exécution des processus et l'activité des AWS API. Activez la protection EKS, la surveillance du temps d'exécution (avec le module complémentaire EKS), ou les deux pour [optimiser la détection des menaces](#). Pour identifier les menaces potentielles, GuardDuty introduit un nouveau type de découverte — [AttackSequence:EKS/CompromisedCluster](#). Pour plus d'informations, consultez la section [Détection étendue des menaces](#).

17 juin 2025

Fonctionnalité mise à jour - Protection contre les logiciels malveillants pour S3

Malware Protection for S3 ne prend pas en charge l'analyse des archives présentant un taux de compression extrêmement élevé. Ces fichiers seront ignorés lors de la numérisation et marqués d'un résultat d'analyse de `UNSUPPORTED`. Pour plus d'informations, consultez la section État [potentiel d'analyse de l'objet S3 et état des résultats](#).

13 juin 2025

[Fonctionnalité mise à jour - Protection contre les logiciels malveillants pour EC2](#)

Malware Protection for EC2 a ajouté la prise en charge de l'analyse de la majorité des instances avec productCo de asmarketplace . Cela s'applique à la fois à l'analyse des GuardDuty-initiated logiciels malveillants et aux analyses des On-demand logiciels malveillants. Pour plus d'informations, consultez la section [Raisons pour lesquelles une ressource est ignorée lors de l'analyse des programmes malveillants.](#)

13 juin 2025

[Nouvelle AmazonGuardDutyFullAccess politique _v2](#)

Ajout d'une nouvelle AmazonGuardDutyFullAccess_v2 politique avec des autorisations pour renforcer la sécurité en limitant les actions administratives aux principaux responsables GuardDuty du service. Pour plus d'informations sur cette stratégie recommandée, voir [AWS Stratégie gérée : AmazonGuardDutyFullAccess_v2.](#)

4 juin 2025

[Support régional étendu pour la protection RDS](#)

GuardDuty La protection RDS est désormais disponible dans les régions du Mexique (centre), de l'Asie-Pacifique (Thaïlande) et de l'Asie-Pacifique (Malaisie). La protection RDS vous aide à détecter les comportements de connexion potentiellement suspects dans les environnements compatibles Aurora MySQL, Aurora PostgreSQL (y compris Limitless Database) et RDS pour PostgreSQL. En cas de détection d'une menace, GuardDuty génère un résultat de protection RDS. Pour plus d'informations sur les bases de données prises en charge et sur l'activation de ce plan de protection dans les nouvelles régions prises en charge, consultez la section [Protection RDS](#).

4 juin 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.7.1 du nouvel agent de sécurité pour les ressources Amazon EC2. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

3 juin 2025

[Support pour la détection](#)
[étendue des menaces](#)

GuardDuty La détection étendue des menaces est désormais disponible en Asie-Pacifique (Thaïlande) (ap-southeast-7). Aucune activation n'est nécessaire, il détecte les attaques en plusieurs étapes qui couvrent les sources de données, plusieurs types de AWS ressources et le temps, au sein d'un Compte AWS. Lorsque des menaces potentielles sont détectées, cela génère une recherche de séquence d'attaque. Pour plus d'informations, consultez la section [Détection étendue des menaces](#).

12 mai 2025

[Support pour la région du Mexique \(centre\)](#)

Amazon GuardDuty est désormais disponible dans la région Mexique (centre) `mx-central-1` (). Pour l'activer GuardDuty dans cette région, consultez la section [Mise en route](#). Vous pouvez recevoir des notifications concernant les mises à jour des GuardDuty fonctionnalités et les détections de menaces en [vous abonnent aux annonces Amazon GuardDuty SNS](#) dans cette région.

7 mai 2025

[Fonctionnalité mise à jour - Surveillance du temps d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.10.0 du nouvel agent de sécurité pour les ressources Amazon EKS. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

4 avril 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitorin
g publie la version 1.7.0 du
nouvel agent de sécurité
pour Amazon ECS-Farga
te Resources. Pour plus
d'informations sur les
nouvelles versions de l'agent
de sécurité et une liste de
ressources supplémentaires
permettant de mettre à jour
votre agent de sécurité,
consultez la section [Versions](#)
[GuardDuty publiées de l'agent](#)
[de sécurité.](#)

4 avril 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitorin
g publie la version 1.7.0 du
nouvel agent de sécurité pour
les ressources Amazon EC2.
Pour plus d'informations sur
les nouvelles versions de
l'agent de sécurité et une liste
de ressources supplémen
taires permettant de mettre à
jour votre agent de sécurité,
consultez la section [Versions](#)
[GuardDuty publiées de l'agent](#)
[de sécurité.](#)

3 avril 2025

Support pour la région Asie-Pacifique (Thaïlande)

Amazon GuardDuty est désormais disponible dans la région Asie-Pacifique (Thaïlande). Pour plus d'informations sur les fonctionnalités prises en charge dans cette région, consultez la section [Disponibilité des Region-specific fonctionnalités](#). Pour l'activer GuardDuty dans cette région, consultez la section [Mise en route](#). Vous pouvez recevoir des notifications concernant les mises à jour des GuardDuty fonctionnalités et les détections de menaces en [vous abonnent aux annonces Amazon GuardDuty SNS](#).

1er avril 2025

Fonctionnalités mises à jour

Le tableau de bord récapitulatif affiche désormais des informations basées sur tous les résultats de sécurité générés, supprimant ainsi la contrainte précédente de 5 000 résultats. Pour plus d'informations sur ces informations, consultez le tableau de [bord GuardDuty récapitulatif](#).

17 mars 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps d'exécution](#)

GuardDuty Runtime Monitoring publie la version 1.9.0 du nouvel agent de sécurité pour les ressources Amazon EKS. Pour plus d'informations sur les nouvelles versions de l'agent de sécurité et une liste de ressources supplémentaires permettant de mettre à jour votre agent de sécurité, consultez la section [Versions GuardDuty publiées de l'agent de sécurité](#).

2 mars 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps d'exécution](#)

GuardDuty Runtime Monitoring a ajouté un nouveau type de problème de couverture (agent non provisionné) pour les ressources Amazon EC2. Pour plus d'informations sur la résolution de ce problème, consultez [Résolution des problèmes de couverture des environnements d'exécution Amazon EC2](#).

21 février 2025

[Fonctionnalité mise à jour](#)
[- Surveillance du temps](#)
[d'exécution](#)

GuardDuty Runtime Monitoring publie de nouveaux agents de sécurité pour Amazon EC2 et Amazon ECS-Fargate Resources. Pour plus d'informations sur les nouvelles versions des agents de sécurité et une liste de ressources supplémentaires permettant de mettre à jour vos agents de sécurité, consultez [GuardDuty la section Versions publiées des agents de sécurité](#).

6 février 2025

[GuardDuty soutien dans la](#)
[région Asie-Pacifique \(Malaisie\)](#)
[\) existante](#)

GuardDuty La détection étendue des menaces est désormais disponible dans la région Asie-Pacifique (Malaisie). Pour plus d'informations, consultez la section [Détection étendue des menaces](#).

28 janvier 2025

[Support pour la région Asie-Pacifique \(Malaisie\)](#)

Amazon GuardDuty est désormais disponible dans la région Asie-Pacifique (Malaisie). Pour plus d'informations sur les fonctionnalités prises en charge dans cette région, consultez la section [Disponibilité des Region-spécific fonctionnalités](#). Pour l'activer GuardDuty dans cette région, consultez la section [Mise en route](#). Vous pouvez recevoir des notifications concernant les mises à jour des GuardDuty fonctionnalités et les détections de menaces en [vous abonnant aux annonces Amazon GuardDuty SNS](#).

16 janvier 2025

[Fonctionnalité mise à jour - Surveillance du temps d'exécution](#)

GuardDuty Runtime Monitoring a mis à jour les informations supplémentaires et les étapes de résolution des problèmes de ECS-Fargate couverture Amazon associés au non-provisionnement de l'agent. Pour plus d'informations sur le type de problème lié à l'agent non provisionné, consultez [Résolution des problèmes liés à la couverture des ECS-Fargate environnements d'exécution Amazon](#).

8 janvier 2025

[Nouveau type de recherche -
Policy:IAMUser/ShortTermRo
tCredentialUsage](#)

GuardDuty introduit un nouveau type de recherche qui vous alerte lorsque des informations d'identification utilisateur restreintes, créées pour les utilisateurs répertoriés Comptes AWS dans votre environnement, sont utilisées pour envoyer des demandes à Services AWS. Pour plus d'informations, consultez [Policy:IAMUser/ShortTermRo
tCredentialUsage](#).

8 janvier 2025

[Nouvelle fonctionnalité -
Détection GuardDuty étendue
des menaces](#)

GuardDuty annonce la détection étendue des menaces pour détecter les séquences d'attaques en plusieurs étapes qui couvrent les sources de données et les AWS ressources GuardDuty fondamentales de votre Compte AWS entreprise, sur une période donnée. Sans frais supplémentaires, cette fonctionnalité est automatiquement activée pour tous les comptes qui l'ont activée GuardDuty. Cette fonctionnalité annonce deux nouveaux types de GuardDuty recherche, appelés types de [recherche de séquences d'attaque](#). Pour plus d'informations, consultez la section [Détection étendue des menaces](#).

1er décembre 2024

[Fonctionnalité multiservice améliorée : surveillance du temps d'exécution et protection contre les logiciels malveillants pour EC2](#)

Impact des nouvelles fonctionnalités d'Amazon Elastic Kubernetes Service (Amazon EKS) sur les fonctionnalités d'Amazon : GuardDuty 1er décembre 2024

- Mode automatique Amazon EKS : la surveillance du temps d'exécution pour Amazon EKS et la protection contre les logiciels malveillants pour EC2 le prennent en charge.
- Nœuds hybrides Amazon EKS : la surveillance du temps d'exécution pour Amazon EKS et la protection contre les logiciels malveillants pour EC2 ne le prennent pas en charge.

Pour plus d'informations, consultez [Comment fonctionne la surveillance du temps d'exécution avec les clusters Amazon EKS et Malware Protection for EC2](#).

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring a publié la version 1.8.1 d'un nouvel agent (v1.8.1-eks-build.2) pour les ressources Amazon EKS. Avec cette nouvelle version de l'agent, la prise en charge de la surveillance du temps d'exécution GuardDuty s'étend aux ressources Amazon EKS qui s'exécutent sur RedHat CentOS et Fedora. Pour plus d'informations, consultez la section [Validation des exigences architecturales](#). Pour plus d'informations sur les notes de publication, consultez les [ressources relatives à l'agent de GuardDuty sécurité pour Amazon EKS](#).

23 novembre 2024

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring a publié une nouvelle version d'agent 1.5.0 pour les ressources Amazon EC2. Cette nouvelle version de l'agent GuardDuty étend la prise en charge de la surveillance du temps d'exécution pour les ressources Amazon EC2 qui s'exécutent sur RedHat CentOS et Fedora. Pour plus d'informations, consultez la section [Validation des exigences architecturales](#). Pour plus d'informations sur les notes de publication, consultez les [GuardDuty ressources relatives à l'agent de sécurité pour Amazon EC2](#).

20 novembre 2024

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring a publié une nouvelle version d'agent 1.5.0 pour Amazon ECS-Fargate Resources. Pour plus d'informations sur les notes de publication, consultez [l'agent de GuardDuty sécurité pour AWS Fargate \(Amazon ECS uniquement\)](#).

14 novembre 2024

[Fonctionnalité mise à jour dans Malware Protection for EC2](#)

7 novembre 2024

GuardDuty Malware Protection for EC2 a ajouté trois types de résultats de surveillance de l'exécution à la liste des [résultats qui appellent une analyse des GuardDuty-initiated programmes malveillants](#) sur les instances Amazon EC2. Les comptes qui ont activé la protection contre les programmes malveillants pour EC2 observent le scan des GuardDuty-initiated programmes malveillants lorsqu'ils GuardDuty génèrent l'un des résultats suivants :

- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

Fonctionnalité mise à jour dans RDS Protection

6 novembre 2024

GuardDuty RDS Protection ajoute la nouvelle 16.4-limitless version du moteur de base de données [Aurora PostgreSQL Limitless](#) à la liste des bases de données prises en charge. Pour Comptes AWS cela, j'ai déjà activé la protection RDS et GuardDuty commencera automatiquement à surveiller le comportement de connexion à la base de données Limitless. Les comptes qui ont déjà utilisé l'essai gratuit de 30 jours de RDS Protection seront soumis à des frais d'utilisation associés à Limitless Database, ainsi qu'aux autres bases de données prises en charge qui sont surveillées. Pour plus d'informations, consultez la section [Protection RDS](#).

[Expansion GuardDuty et AWS PrivateLink intégration de la région](#)

GuardDuty étend désormais le support régional pour [Amazon GuardDuty et les points de terminaison VPC d'interface](#) (). AWS PrivateLink. Auparavant, le support régional était disponible pour l'est des États-Unis (Virginie du Nord), l'Europe (Irlande) et Israël (Tel Aviv). Ce support est désormais étendu à tous les Régions AWS endroits où il GuardDuty est disponible. Pour plus d'informations sur les différences régionales, consultez la section [Disponibilité des Region-specific fonctionnalités](#).

6 novembre 2024

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring a publié la version 1.4.1 d'un nouvel agent pour Amazon ECS-Fargate Resources. Pour plus d'informations sur les notes de publication, consultez [l'agent de GuardDuty sécurité pour AWS Fargate \(Amazon ECS uniquement\)](#).

24 octobre 2024

[Ajout du support pour les opérations de GuardDuty CloudFormation balises](#)

GuardDuty prend désormais en charge la mise à jour de la clé et de la valeur des balises, ainsi que des balises au niveau de la pile. Pour ce faire, ajoutez une autorisation guarddduty :tagResource au rôle IAM. Pour plus d'informations GuardDuty CloudFormation, consultez la [référence aux types de GuardDuty ressources Amazon](#) dans le guide de AWS CloudFormation l'utilisateur.

24 octobre 2024

[Fonctionnalité mise à jour dans GuardDuty Malware Protection for S3](#)

Lorsque vous activez la protection contre les programmes malveillants pour S3, vous pouvez choisir un rôle de service disposant des autorisations nécessaires pour effectuer des actions d'analyse des programmes malveillants en votre nom. Pour plus d'informations sur l'activation de la protection contre les programmes malveillants pour S3, consultez [la section Configuration de la protection contre les programmes malveillants pour S3 pour votre compartiment S3](#).

22 octobre 2024

Fonctionnalités mises à jour

GuardDuty améliore le type de [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#) recherche pour détecter l'utilisation des informations d' AWS identification d'instance Amazon EC2 provenant de points de terminaison VPC (AWS PrivateLink) Comptes AWS qui ne sont pas associés au rôle d'instance Amazon EC2. Cette nouvelle GuardDuty fonctionnalité détecte une éventuelle utilisation abusive des informations d'identification de l'instance Amazon EC2 et fournit le contexte de la télécommande à l' Compte AWS aide des informations d'identification de session d'exfiltration. Pour plus d'informations sur les points AWS de terminaison de service pris en charge par cette nouvelle détection, consultez la section [Journalisation des événements d'activité réseau](#) dans le guide de AWS CloudTrail l'utilisateur.

21 octobre 2024

[Fonctionnalité mise à jour - Surveillance du GuardDuty temps d'exécution](#)

GuardDuty Runtime Monitoring a ajouté les trois types de résultats suivants qui vous avertissent lorsque des commandes suspectes sont exécutées sur une instance Amazon EC2 ou une charge de travail de conteneur au sein de votre AWS environnement :

10 octobre 2024

- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

[Nouvelle fonctionnalité - Ajout de la prise en charge des points de terminaison VPC](#)

GuardDuty est désormais intégré aux points de terminaison VPC AWS PrivateLink et les prend en charge. Pour plus d'informations sur l'AWS PrivateLink intégration, consultez [Amazon GuardDuty et interface VPC endpoints](#) ().AWS PrivateLink

17 septembre 2024

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring a publié la version 1.7.1 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour Amazon EKS](#).

13 septembre 2024

[Fonctionnalité mise à jour dans Malware Protection for S3](#)

Malware Protection for S3 a ajouté un nouveau champ `s3Throttled`, au schéma Amazon EventBridge (EventBridge) des résultats d'analyse des objets S3. Le `s3Throttled` champ indique s'il y a eu un retard dans le chargement ou la récupération du stockage à partir des buckets Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez la section [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).

13 septembre 2024

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring a publié la version 1.3.1 d'un nouvel agent pour les ressources Amazon EC2. Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour Amazon EC2](#).

12 septembre 2024

[Fonctionnalités mises à jour dans Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring a publié la version 1.3.1 d'un nouvel agent pour Amazon ECS-Fargate Resources. Pour plus d'informations sur les notes de publication, consultez [l'agent de GuardDuty sécurité pour AWS Fargate \(Amazon ECS uniquement\)](#).

11 septembre 2024

Rôle GuardDuty lié à un service (SLR) mis à jour

GuardDuty a mis à jour le SLR pour inclure l'ec2:DescribeVpcs autorisation dans les actions Amazon EC2. Pour plus d'informations, consultez la section [Autorisations de Service-linked rôle pour GuardDuty](#).

22 août 2024

Ajout de contenu significatif

GuardDuty a ajouté des mises à jour de contenu importantes à la fonctionnalité Malware Protection for S3.

20 août 2024

- Ajout de nouveaux exemples de schéma de notification pour configurer les EventBridge règles Amazon afin de recevoir des notifications relatives à l'état des ressources du plan de protection contre les logiciels malveillants et au résultat de l'analyse des objets S3. Pour plus d'informations, consultez la section [Surveillance des scans d'objets S3 avec Amazon EventBridge](#).
- Ajout d'informations sur le [dépannage des défaillances des balises après le scan des objets S3](#).

[Fonctionnalités mises à jour dans GuardDuty Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring a publié la version 1.3.0 d'un nouvel agent pour les ressources Amazon EC2. Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour Amazon EC2](#).

19 août 2024

[Fonctionnalités mises à jour dans GuardDuty Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring a publié la version 1.7.0 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour les clusters Amazon EKS](#).

17 août 2024

[Ajout de contenu significatif](#)

GuardDuty a ajouté de nouvelles informations sur la méthodologie de détection des programmes malveillants et les moteurs d'analyse utilisés pour les fonctionnalités Malware Protection for S3 et Malware Protection for EC2. Pour plus d'informations, consultez la section [Moteur d'analyse pour la détection des GuardDuty programmes malveillants](#).

15 août 2024

[Nouvelle fonctionnalité - Protection des charges de travail liées à l'IA](#)

GuardDuty la détection des menaces fondamentales et la protection Lambda vous aident à mieux sécuriser et détecter les menaces qui pèsent sur les charges de travail basées sur l'IA. AWS Pour plus d'informations, consultez la section [Protection des charges de travail basées sur l'IA avec GuardDuty](#).

14 août 2024

[Fonctionnalité mise à jour dans GuardDuty Runtime Monitoring - Fargate \(Amazon ECS uniquement\)](#)

Runtime Monitoring a publié une nouvelle version d'agent 1.3.0 pour les ressources AWS Fargate (Amazon ECS uniquement). Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour Fargate-ECS](#).

9 août 2024

[Fonctionnalité mise à jour - Protection contre les logiciels malveillants pour S3](#)

GuardDuty Malware Protection for S3 augmente le quota maximal de compartiments S3 de 10 à 25 compartiments. Ce quota s'applique à un Compte AWS pour chaque personne Région AWS. Pour plus d'informations, consultez la section [Protection contre les programmes malveillants pour S3](#).

8 août 2024

[Mise à jour - Nouveaux types de recherche dans Runtime Monitoring](#)

GuardDuty a ajouté deux nouveaux types de détection de la surveillance du temps d'exécution qui vous aideront à détecter les menaces impliquant la création d'un shell suspect sur la ressource surveillée et l'augmentation des privilèges lorsqu'un processus élève de manière suspecte ses privilèges au rang de root.

6 août 2024

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[Mis à jour - Intégration avec AWS Security Hub CSPM](#)

AWS Security Hub CSPM fournit une liste de contrôles de GuardDuty sécurité pour évaluer vos ressources et vérifier votre conformité par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Pour plus d'informations, consultez la section [Utilisation GuardDuty des contrôles dans Security Hub CSPM](#).

11 juillet 2024

[Script de GuardDuty test mis à jour pour les résultats](#)

GuardDuty prend désormais en charge plus de 100 résultats avec différentes AWS ressources dans un compte dédié. Pour plus d'informations, consultez la section [GuardDuty Résultats des tests dans des comptes dédiés.](#)

28 juin 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié la version 1.2.0 d'un nouvel agent de sécurité pour la ressource Amazon EC2. Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour l'instance Amazon EC2.](#) Pour plus d'informations sur la mise à jour manuelle de l'agent de sécurité vers cette version, consultez [Gestion manuelle de l'agent de sécurité pour l'instance Amazon EC2.](#)

13 juin 2024

[Nouvelle fonctionnalité](#)
[- Protection contre les programmes malveillants pour la disponibilité dans la région S3](#)

GuardDuty Malware Protection for S3 est désormais disponible dans toutes les régions commerciales où elle GuardDuty est disponible. Cette fonctionnalité vous permet de scanner les objets récemment chargés dans les compartiments Amazon S3 afin de détecter d'éventuels malwares ou chargements suspects, et de prendre des mesures pour les isoler avant qu'ils ne soient ingérés dans les processus en aval. Pour plus d'informations sur l'activation de la protection contre les programmes malveillants pour S3, consultez la section [Protection contre les GuardDuty programmes malveillants pour S3](#).

12 juin 2024

[Nouvelle fonctionnalité - Protection contre les logiciels malveillants pour S3](#)

11 juin 2024

GuardDuty annonce la disponibilité générale de Malware Protection for S3, qui vous aide à analyser les objets récemment chargés dans les compartiments Amazon S3 pour détecter d'éventuels malwares ou chargements suspects, et à prendre des mesures pour les isoler avant qu'ils ne soient ingérés dans les processus en aval. Cette fonctionnalité est entièrement gérée par AWS. GuardDuty publie le résultat de l'analyse des objets S3 sur votre bus d'événements EventBridge par défaut. Vous pouvez GuardDuty autoriser l'ajout de balises à vos objets S3 numérisés. Vous pouvez créer des flux de travail en aval, tels que l'isolation dans un compartiment de quarantaine, ou définir des politiques de compartiment à l'aide de balises qui empêchent les utilisateurs ou les applications d'accéder à certains objets. Pour plus d'informations, consultez la section [Protection contre les GuardDuty programmes malveillants pour S3](#). Il est actuellement disponible dans les régions suivantes :

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Oregon)
- Europe (Irlande)
- Europe (Francfort)
- Europe (Stockholm)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)
- Asie-Pacifique (Singapour)

[Politique AmazonGuardDutyFullAccess mise à jour](#)

Autorisation ajoutée qui vous permet de transmettre un rôle IAM GuardDuty lorsque vous activez Malware Protection pour S3. Pour plus d'informations sur cette mise à jour de politique, voir [Stratégie AWS gérée : AmazonGuardDutyFullAccess](#).

10 juin 2024

[Fonctionnalité mise à jour
dans GuardDuty RDS
Protection](#)

RDS Protection étend le support pour surveiller l'activité de connexion sur vos bases de données RDS pour PostgreSQL. Dans le cadre de cette extension, GuardDuty nous commencerons automatiquement à surveiller les données de connexion des bases de données RDS pour PostgreSQL pour les comptes qui ont déjà activé la protection RDS. GuardDuty Pour plus d'informations, consultez la section [Protection RDS](#).

6 juin 2024

[Fonctionnalité mise à jour
dans GuardDuty Runtime
Monitoring - Fargate \(Amazon
ECS uniquement\)](#)

Runtime Monitoring a publié une nouvelle version d'agent 1.2.0 pour les ressources AWS Fargate (Amazon ECS uniquement). Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour Fargate-ECS](#).

31 mai 2024

[Fonctionnalité mise à jour dans GuardDuty Malware Protection for EC2](#)

Pour chaque volume Amazon EBS attaché à vos instances Amazon EC2 et à vos charges de travail de conteneur GuardDuty , Malware Protection for EC2 a augmenté la taille du volume EBS qu'il analyse jusqu'à 2 048 Go. Pour plus d'informations sur l'analyse des volumes Amazon EBS attachés à vos instances, consultez [GuardDuty Malware Protection for EC2](#).

29 mai 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring for Amazon ECS-Fargate Resources permet désormais de détecter les menaces potentielles sur vos tâches lancées par AWS Batch et AWS CodePipeline. Pour plus d'informations, consultez [Comment fonctionne la surveillance du temps d'exécution avec Fargate \(Amazon ECS uniquement\)](#).

28 mai 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié la version 1.6.1 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations sur les notes de mise à jour, consultez [l'historique des versions de l'agent complémentaire EKS](#).

14 mai 2024

[Support régional étendu pour la surveillance du temps d'exécution](#)

GuardDuty étend le soutien à la surveillance du temps d'exécution à la région de l'Ouest du Canada (Calgary) . Pour plus d'informations sur la mise en route de la surveillance du temps d'exécution, voir [Activation de la surveillance du temps d'exécution](#).

7 mai 2024

[Support régional étendu pour la protection RDS](#)

GuardDuty étend la prise en charge de la protection RDS aux éléments suivants : Régions AWS

3 mai 2024

- Canada-Ouest (Calgary)
- Asie-Pacifique (Hyderabad)
- Europe (Espagne)
- Europe (Zurich)
- Moyen-Orient (EAU)
- Israël (Tel Aviv)
- Asie-Pacifique (Melbourne)

Pour plus d'informations sur l'activation de cette fonctionnalité, consultez la section [Protection RDS](#).

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié une nouvelle version d'agent 1.1.0 pour les ressources AWS Fargate (Amazon ECS uniquement). Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour Fargate-ECS](#).

1 mai 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié la version 1.6.0 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations sur les notes de mise à jour, consultez [l'historique des versions de l'agent complémentaire EKS](#).

29 avril 2024

[Support pour IPAddressV6](#)

GuardDuty a ajouté le support IPAddressv6 pour les détails IP locaux et distants. Vous pouvez utiliser les [attributs de filtre](#) associés pour filtrer GuardDuty les résultats ou [créer des règles de suppression](#).

18 avril 2024

[Expérience de console mise à jour pour configurer l'exportation des résultats](#)

GuardDuty a mis à jour l'expérience de la console pour exporter les résultats générés dans votre Comptes AWS compartiment Amazon S3. Pour plus d'informations, consultez la section [Exportation GuardDuty des résultats](#).

1er avril 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié la version 1.1.0 d'un nouvel agent de sécurité pour la ressource Amazon EC2. Cette version prend en charge la configuration GuardDuty automatique des agents dans Runtime Monitoring pour les instances Amazon EC2. Pour plus d'informations sur les notes de publication, consultez [l'agent GuardDuty de sécurité pour l'instance Amazon EC2.](#)

28 mars 2024

[Disponibilité générale de la surveillance du temps d'exécution pour les instances Amazon EC2](#)

28 mars 2024

GuardDuty annonce la disponibilité générale (GA) de la surveillance du temps d'exécution pour les instances Amazon EC2. Vous avez désormais la possibilité d'[activer la configuration automatique de l'agent](#) qui permet GuardDuty d'installer et de gérer l'agent de sécurité pour vos instances Amazon EC2 en votre nom. Avec l'agent GuardDuty automatisé, vous pouvez également utiliser des balises d'inclusion ou d'exclusion GuardDuty pour indiquer d'installer et de gérer l'agent de sécurité uniquement sur certaines instances Amazon EC2. Pour plus d'informations, consultez [Comment la surveillance du temps d'exécution fonctionne avec les instances Amazon EC2](#).

Liste des nouveaux types de trouvailles publiés en même temps que cette AG

- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)

- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)

[Amazon GuardDuty a mis à jour le Service-linked rôle \(SLR\)](#)

26 mars 2024

Utilisez AWS Systems Manager des actions pour gérer les associations SSM sur les instances Amazon EC2 lorsque vous GuardDuty activez la surveillance du temps d'exécution avec un agent automatisé pour Amazon EC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les instances EC2 dotées d'une balise d'inclusion (GuardDuty Managed :true).

- La liste suivante indique les nouvelles autorisations :

```
"ssm:DescribeAssociation",  
"ssm:DeleteAssociation",  
"ssm:UpdateAssociation",  
"ssm:CreateAssociation",  
"ssm:StartAssociationsOnce",  
"ssm:AddTagsToResource",  
"ssm:CreateAssociation",  
"ssm:UpdateAssociation",  
"ssm:SendCommand",
```

```
"ssm:GetCommandInvocation"
```

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Avec la dernière version v1.5.0 de l'agent de GuardDuty sécurité (module complémentaire) pour Amazon EKS, Runtime Monitoring prend désormais en charge la configuration de paramètres spécifiques de votre agent de GuardDuty sécurité, tels que les paramètres du processeur et de la mémoire, PriorityClass les paramètres et les paramètres de politique DNS. Pour plus d'informations, voir [Configuration des paramètres GuardDuty de l'agent de sécurité \(module complémentaire EKS\)](#).

07 mars 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié une nouvelle version d'agent 1.5.0 pour les ressources Amazon EKS. Pour plus d'informations sur les notes de mise à jour, consultez [l'historique des versions de l'agent complémentaire EKS](#).

07 mars 2024

[Support pour le Canada-Ouest \(Calgary\)](#)

Amazon GuardDuty est désormais disponible dans la région de l'Ouest du Canada (Calgary). Certains des plans de protection proposés GuardDuty peuvent ne pas être disponibles dans cette région. Pour obtenir les dernières informations, consultez la section [Régions et points de terminaison](#).

6 mars 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Les versions 1.0.0 et 1.1.0 de l'agent de GuardDuty sécurité pour les clusters Amazon EKS ne seront plus prises en charge à compter du 14 mai 2024. Pour plus d'informations sur les étapes à suivre avant la fin du support standard, consultez l'[agent GuardDuty de sécurité pour les clusters Amazon EKS](#).

16 février 2024

Fonctionnalité mise à jour dans Runtime Monitoring

Runtime Monitoring prend en charge la dernière [version 1.29 de Kubernetes avec la version 1.4.1](#) de l'agent de sécurité existant. Le support est disponible depuis le lancement de cette version de Kubernetes. Pour plus d'informations sur les versions de Kubernetes prises en charge, consultez la section Versions de [Kubernetes](#) prises en charge par l'agent de sécurité. GuardDuty

16 février 2024

[Fonctionnalité mise à jour
dans Runtime Monitoring -
Disponibilité régionale](#)

GuardDuty Runtime Monitoring prend désormais en charge le partage d'Amazon VPC au sein de celui-ci. AWS Organizations GuardDuty le [rôle lié à un service \(SLR\)](#) dispose d'une nouvelle autorisation, `organizations:DescribeOrganization` qui permet de récupérer l'identifiant de l'organisation pour le compte Amazon VPC partagé afin de définir la politique du point de terminaison. Pour plus d'informations sur les conditions préalables à l'utilisation d'un point de terminaison Amazon VPC partagé dans le cadre de la surveillance du temps d'exécution, consultez [Support pour le partage d'Amazon VPC](#). Cette fonctionnalité est disponible dans toutes les régions où la surveillance du temps d'exécution est prise GuardDuty en charge.

12 février 2024

[Fonctionnalité mise à jour dans Runtime Monitoring - Disponibilité régionale](#)

GuardDuty Runtime Monitoring prend désormais en charge le partage d'Amazon VPC au sein de celui-ci. AWS Organizations GuardDuty le [rôle lié à un service \(SLR\)](#) dispose d'une nouvelle autorisation, `organizations:DescribeOrganization` qui permet de récupérer l'identifiant de l'organisation pour le compte Amazon VPC partagé afin de définir la politique du point de terminaison. Pour plus d'informations sur les conditions préalables à l'utilisation d'un point de terminaison Amazon VPC partagé dans le cadre de la surveillance du temps d'exécution, consultez [Support pour le partage d'Amazon VPC](#). Actuellement, cette fonctionnalité est disponible dans certains des Régions AWS. Pour plus d'informations, consultez [Régions et points de terminaison](#).

9 février 2024

[Fonctionnalité mise à jour avec prise en charge de la nouvelle version Régions AWS : Malware Protection for EC2](#)

Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés Clés gérées par AWS dans la région de l'ouest des États-Unis (Oregon).

6 février 2024

[Fonctionnalité mise à jour avec prise en charge de la nouvelle version Régions AWS : Malware Protection for EC2](#)

[Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés avec Clés gérées par AWS les méthodes suivantes : Régions AWS](#)

5 février 2024

- Asie-Pacifique (Singapour) (ap-southeast-1)
- Europe (Francfort) (eu-central-1)
- Asie-Pacifique(Osaka) (ap-northeast-3)
- USA Est (Ohio) (us-east-2)
- Europe (Milan) (eu-south-1)
- Asie-Pacifique (Tokyo) (ap-northeast-1)
- Asie-Pacifique (Séoul) (ap-northeast-2)
- Canada (Centre) (ca-central-1)
- Europe (Irlande) (eu-west-1)
- USA Est (Virginie du Nord) (us-east-1)

Fonctionnalité mise à jour dans Runtime Monitoring

GuardDuty Runtime Monitoring a publié une nouvelle version GuardDuty de l'agent de sécurité (v1.0.2) pour les instances Amazon EC2. Cette version de l'agent inclut la prise en charge des dernières AMI Amazon ECS. Pour plus d'informations sur l'historique des versions de l'agent, consultez [GuardDuty la section Agent de sécurité pour les instances Amazon EC2.](#)

2 février 2024

[Fonctionnalité mise à jour avec prise en charge de la nouvelle version Régions AWS : Malware Protection for EC2](#)

[Malware Protection for EC2 prend désormais en charge l'analyse des volumes Amazon EBS chiffrés avec Clés gérées par AWS les méthodes suivantes : Régions AWS](#)

31 janvier 2024

- Europe (Londres) (eu-west-2)
- Europe (Stockholm) (eu-north-1)
- Asie-Pacifique (Hong Kong) (ap-east-1)
- Afrique (Le Cap) (af-south-1)
- Moyen-Orient (Bahreïn) (me-south-1)
- Asie-Pacifique (Hyderabad) (ap-south-2)
- Europe (Espagne) (eu-south-2)
- Asie-Pacifique (Melbourne) (ap-southeast-4)
- Asie-Pacifique (Sydney) (ap-southeast-2)
- Israël (Tel Aviv) (il-central-1)

[Mise à jour de la gestion des comptes avec AWS Organizations](#)

Réorganisation du contenu sous [Gestion des comptes avec AWS Organizations](#). , a ajouté des étapes pour modifier le compte d' GuardDuty administrateur délégué et a mis à jour [Comprendre la relation entre le compte d' GuardDuty administrateur et les comptes de membre](#).

30 janvier 2024

[Fonctionnalité mise à jour avec prise en charge de nouvelles Régions AWS](#)

[Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés avec Clés gérées par AWS les méthodes suivantes : Régions AWS](#)

29 janvier 2024

- Asie-Pacifique (Jakarta) (ap-southeast-3)
- USA Ouest (Californie du Nord) (us-west-1)
- Moyen-Orient (EAU) (me-central-1)
- Europe (Zurich) (eu-central-2)
- Asie-Pacifique (Mumbai) (ap-south-1)
- Amérique du Sud (Sao Paulo) (sa-east-1)

[Fonctionnalité mise à jour dans Malware Protection for EC2](#)

25 janvier 2024

Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés à l'aide de Clés gérées par AWS [Malware Protection for EC2 service-linked role \(SLR\)](#) dispose de deux nouvelles autorisations : `GetSnapshotBlock` et `ListSnapshotBlocks`

Ces autorisations vous aideront à GuardDuty récupérer l'instantané d'un volume EBS (chiffré à l'aide de Clé gérée par AWS) sur votre compte de service Compte AWS et à le copier sur le [compte de GuardDuty service](#) avant de lancer l'analyse des logiciels malveillants. Actuellement, cette fonctionnalité n'est disponible qu'en Europe (Paris-west-3) (). Pour plus d'informations, consultez la section [Volumes pris en charge pour l'analyse des programmes malveillants](#).

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

GuardDuty Runtime Monitoring a publié une nouvelle version GuardDuty de l'agent de sécurité (v1.0.1) avec des optimisations et des améliorations générales des performances. Pour plus d'informations sur l'historique des versions de l'agent, consultez [GuardDuty la section Agent de sécurité pour les instances Amazon EC2.](#)

23 janvier 2024

[Fonctionnalité mise à jour dans Runtime Monitoring](#)

Runtime Monitoring a publié la version 1.4.1 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations, veuillez consulter [Historique des versions de l'agent de module complémentaire EKS](#) (langue française non garantie).

16 janvier 2024

[Runtime Monitoring a publié un nouvel agent v1.4.0 pour les ressources Amazon EKS](#)

Runtime Monitoring a publié la version 1.4.0 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations, veuillez consulter [Historique des versions de l'agent de module complémentaire EKS](#) (langue française non garantie).

21 décembre 2023

[Ajout de types de résultats basés sur le S3 et l'apprentissage AWS CloudTrail automatique \(ML\) en Europe \(Zurich\), en Europe \(Espagne\), en Asie-Pacifique \(Hyderabad\), en Asie-Pacifique \(Melbourne\) et en Israël \(Tel Aviv\)](#)

21 décembre 2023

Le S3 et les CloudTrail résultats suivants qui identifient le comportement anormal à l'aide GuardDuty du modèle d'apprentissage automatique (ML) de détection des anomalies sont désormais disponibles dans les régions d'Europe (Zurich), d'Europe (Espagne), d'Asie-Pacifique (Hyderabad), d'Asie-Pacifique (Melbourne) et d'Israël (Tel Aviv) :

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)

- [Persistence:IAMUser/
AnomalousBehavior](#)
- [PrivilegeEscalation:IAMUser/
AnomalousBehavior](#)
- [Discovery:IAMUser/
AnomalousBehavior](#)

[GuardDuty prend en charge
50 000 comptes membres via
AWS Organizations](#)

Un GuardDuty administrateur délégué peut désormais gérer un maximum de 50 000 comptes de membres via AWS Organizations. Cela inclut également un maximum de 5 000 comptes membres associés au compte GuardDuty administrateur sur invitation.

20 décembre 2023

[GuardDuty Support de surveillance du temps d'exécution étendu à 19 Régions AWS](#)

La surveillance du temps d'exécution est désormais disponible en Asie-Pacifique (Jakarta), en Europe (Paris), en Asie-Pacifique (Osaka), en Asie-Pacifique (Séoul), au Moyen-Orient (Bahreïn), en Europe (Espagne), en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Melbourne), en Israël (Tel Aviv), dans l'ouest des États-Unis (Californie du Nord), en Europe (Londres), en Asie-Pacifique (Hong Kong), en Europe (Milan), au Moyen-Orient (Émirats arabes unis), Amérique du Sud (São Paulo), Asie-Pacifique (Mumbai), Canada (Centre), Afrique (Le Cap), Europe (Zurich).

6 décembre 2023

[GuardDuty étend la capacité de surveillance du temps d'exécution](#)

26 novembre 2023

Outre la détection des menaces qui pèsent sur vos clusters Amazon EKS, GuardDuty annonce la disponibilité générale de Runtime Monitoring pour détecter les menaces pesant sur vos charges de travail Amazon ECS et d'une version préliminaire pour détecter les menaces visant vos instances Amazon EC2. Pour plus d'informations sur ceux qui prennent Régions AWS actuellement en charge la surveillance du temps d'exécution, voir [Régions et points de terminaison](#).

[Amazon GuardDuty a mis à jour le Service-linked rôle \(SLR\)](#)

26 novembre 2023

GuardDuty a ajouté de nouvelles autorisations permettant d'utiliser les actions Amazon ECS pour gérer et récupérer des informations sur les clusters Amazon ECS, et de gérer les paramètres du compte Amazon ECS avec `guardduty:Activate`. Les actions relatives à Amazon ECS récupèrent également les informations relatives aux balises associées à GuardDuty.

- Les autorisations suivantes ont été ajoutées dans le cadre de l'extension de la fonctionnalité de [surveillance du temps d'exécution](#) :

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

[Mise à jour des politiques AWS gérées](#)

16 novembre 2023

GuardDuty a ajouté une nouvelle autorisation, `organizations:ListAccounts` à la [politique AWS gérée : AmazonGuardDutyFullAccess](#) et [AmazonGuardDutyReadOnlyAccess](#).

[GuardDuty a publié de nouveaux types de résultats qui utilisent EKS Audit Log Monitoring.](#)

EKS Audit Log Monitoring prend désormais en charge les types de résultats suivants en Asie-Pacifique (Melbourne) (ap-southeast-4).

11 novembre 2023

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty a publié de nouveaux types de résultats qui utilisent EKS Audit Log Monitoring.](#)

10 novembre 2023

EKS Audit Log Monitoring prend désormais en charge les types de résultats suivants dans les régions Asie-Pacifique (Hyderabadap-south-2) (), Europe (Zurich eu-central-2) () et Europe (Espagne) (eu-south-2).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

- Discovery:Kubernetes/
AnomalousBehavior.Permis
sionChecked

[GuardDuty a publié de nouveaux types de résultats qui utilisent EKS Audit Log Monitoring.](#)

8 novembre 2023

EKS Audit Log Monitoring prend désormais en charge les types de résultats suivants. Ces types de recherche ne sont pas encore disponibles dans les régions Asie-Pacifique (Hyderabadap-south-2), Europe (Zurich eu-central-2), Europe (Espagne) (eu-south-2) et Asie-Pacifique (Melbourne) (ap-southeast-4).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[La surveillance d'exécution
EKS a publié un nouvel agent
version 1.3.1](#)

EKS Runtime Monitoring a publié une nouvelle version d'agent 1.3.1 qui inclut d'importants correctifs et mises à jour de sécurité.

23 octobre 2023

[Nouvel attribut de filtre pour le
résultat](#)

GuardDuty a ajouté un nouveau critère pour filtrer les résultats générés. Le suffixe de domaine de requête DNS fournit le domaine de deuxième et de premier niveau impliqué dans l'activité GuardDuty à l'origine de la recherche.

17 octobre 2023

[La surveillance d'exécution
EKS a publié un nouvel agent
version 1.3.0 compatible avec
Kubernetes version 1.28](#)

EKS Runtime Monitoring a publié une nouvelle version d'agent 1.3.0 qui prend en charge la version 1.28 de Kubernetes. Ajout de la prise en charge d'Ubuntu Pour plus d'informations, veuillez consulter [Historique des versions de l'agent de module complémentaire EKS](#) (langue française non garantie).

5 octobre 2023

[Ajout de types de résultats basés sur S3 et l'apprentissage AWS CloudTrail automatique \(ML\) dans les régions Asie-Pacifique \(Jakarta\) et Moyen-Orient \(Émirats arabes unis\)](#)

20 septembre 2023

Le S3 et les CloudTrail résultats suivants qui identifient le comportement anormal à l'aide GuardDuty du modèle d'apprentissage automatique (ML) de détection des anomalies sont désormais disponibles dans les régions Asie-Pacifique (Jakarta) et Moyen-Orient (Émirats arabes unis) :

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)

- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)

[GuardDuty EKS Runtime Monitoring introduit GuardDuty la gestion des agents de sécurité au niveau du cluster](#)

EKS Runtime Monitoring prend en charge la gestion de l'agent de GuardDuty sécurité pour les clusters EKS individuels afin de surveiller les événements d'exécution provenant uniquement de ces clusters sélectifs. La surveillance d'exécution EKS étend cette fonctionnalité avec la prise en charge des balises.

13 septembre 2023

[GuardDuty Malware Protection for EC2 étend le support à un plus grand nombre Régions AWS](#)

Malware Protection for EC2 est désormais disponible en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Melbourne), en Europe (Zurich) et en Europe (Espagne).

11 septembre 2023

[GuardDuty est désormais disponible dans la région Israël \(Tel Aviv\)](#)

24 août 2023

La région d'Israël (Tel Aviv) a été ajoutée à la liste Régions AWS GuardDuty des régions désormais disponibles. Les plans de protection suivants sont également disponibles dans la région Israël (Tel Aviv) :

- [Protection EKS](#) inclut la surveillance des journaux d'audit EKS et la surveillance d'exécution EKS.
- [Protection Lambda](#).
- [Protection contre les logiciels malveillants pour EC2](#).
- [Protection S3](#).

Pour plus d'informations sur la disponibilité des plans de protection dans la région Israël (Tel Aviv), veuillez consulter [Régions et points de terminaison](#).

[GuardDuty ajout d'une configuration d'activation automatique pour votre organisation au niveau du plan de protection](#)

Mettez à jour la configuration organisationnelle des plans de protection de votre région. Les options de configuration possibles sont soit l'activation pour tous les comptes, soit l'activation automatique pour les nouveaux comptes, soit l'activation automatique pour aucun des comptes de votre organisation.

16 août 2023

[Les types de recherche S3 qui identifient les comportements anormaux à l'aide GuardDuty du modèle d'apprentissage automatique \(ML\) de détection des anomalies sont désormais disponibles en Asie-Pacifique \(Osaka\)](#)

Les types de résultat suivants sont disponibles dans la région Asie-Pacifique (Osaka) :

10 août 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[La surveillance d'exécution EKS est désormais disponible en Asie-Pacifique \(Melbourne\)](#)

La surveillance du temps d'exécution GuardDuty EKS intégrée à EKS Protection permet de détecter les menaces d'exécution pour vos clusters Amazon EKS dans votre AWS environnement. Elle est désormais prise en charge dans la région Asie-Pacifique (Melbourne).

08 août 2023

[Mise à jour de la liste des GuardDuty résultats qui déclenchent une analyse des GuardDuty-initiated programmes malveillants](#)

Certains types de détection d'EKS Runtime Monitoring peuvent désormais déclencher GuardDuty-initiated une analyse des logiciels malveillants dans votre Compte AWS.

19 juillet 2023

[GuardDuty prend en charge 10 000 comptes membres via AWS Organizations](#)

Un compte GuardDuty administrateur peut désormais gérer un maximum de 10 000 comptes de membres via AWS Organizations. Cela inclut également un maximum de 5 000 comptes membres associés au compte GuardDuty administrateur sur invitation.

29 juin 2023

[La surveillance d'exécution EKS annonce trois nouveaux types de résultat.](#)

La surveillance d'exécution EKS prend en charge trois nouveaux types de résultat basés sur la technique d'injection de processus. Les nouveaux types de recherche sont DefenseEvasion:Runtime/ProcessInjection.Proc DefenseEvasion:Runtime/ProcessInjection.Ptrace, et DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.

22 juin 2023

[La surveillance d'exécution EKS a publié un nouvel agent version 1.2.0 compatible avec Kubernetes version 1.27](#)

EKS Runtime Monitoring a publié une nouvelle version d'agent 1.2.0 qui prend également en charge les ARM64-based instances. Ajout de la prise en charge de Bottlerocket. Pour plus d'informations, veuillez consulter [Historique des versions de l'agent de module complémentaire EKS](#) (langue française non garantie).

16 juin 2023

[GuardDuty la console fournit une vue résumée de vos résultats.](#)

Le tableau de bord récapitulatif de la GuardDuty console fournit une vue agrégée des GuardDuty résultats. Actuellement, le tableau de bord affiche les données via différents widgets pour les 10 000 dernières découvertes générées pour votre compte (ou les comptes de membre si vous êtes un compte GuardDuty administrateur) pour la région actuelle.

12 juin 2023

[La surveillance des journaux d'audit EKS est désormais disponible dans les régions Asie-Pacifique \(Hyderabad\), Asie-Pacifique \(Melbourne\), Europe \(Zurich\) et Europe \(Espagne\).](#)

Activez la surveillance des journaux d'audit EKS (dans EKS Protection) pour que vos comptes surveillent les journaux d'audit EKS de vos clusters Amazon EKS et les analysent pour détecter toute activité potentiellement malveillante et suspecte.

1er juin 2023

[La surveillance des journaux d'audit EKS est désormais disponible dans la région Moyen-Orient \(EAU\).](#)

EKS Audit Log Monitoring est désormais disponible au Moyen-Orient (Émirats arabes unis). Activez la surveillance des journaux d'audit EKS pour vos comptes afin de surveiller les journaux d'audit EKS de vos clusters Amazon EKS et de les analyser pour détecter toute activité potentiellement malveillante et suspecte.

3 mai 2023

[GuardDuty Malware Protection for EC2 annonce une analyse des On-demand malwares](#)

27 avril 2023

Malware Protection for EC2 vous aide à détecter la présence potentielle de programmes malveillants dans les volumes Amazon EBS attachés à vos instances Amazon EC2 et à vos charges de travail de conteneur. Il propose désormais deux types de scans : GuardDuty initiés et à la demande. GuardDuty-initiated l'analyse des programmes malveillants lance automatiquement une analyse sans agent dans les volumes Amazon EBS uniquement lorsqu'elle GuardDuty génère l'un des [résultats invoquant GuardDuty-initiated](#) une analyse des programmes malveillants. Vous pouvez lancer une analyse des On-demand programmes malveillants pour les instances Amazon EC2 de votre compte en fournissant le nom de ressource Amazon (ARN) associé à cette instance Amazon EC2. Pour plus d'informations sur les différences entre les deux types de scan, consultez [Malware Protection for EC2](#).

- [GuardDuty-initiated analyse des logiciels malveillants](#)

	<ul style="list-style-type: none">• On-demand analyse des logiciels malveillants	
GuardDuty annonce Lambda Protection	<p>La protection Lambda vous aide à identifier les menaces de sécurité potentielles dans vos fonctions AWS Lambda .</p>	20 avril 2023
	<ul style="list-style-type: none">• Types de résultat de la protection Lambda• Corriger une fonction Lambda potentiellement compromise	
GuardDuty est désormais disponible dans la région Asie-Pacifique (Melbourne)	<p>La région Asie-Pacifique (Melbourne) a été ajoutée à la liste Régions AWS des GuardDuty destinations disponibles. Pour plus d'informations sur les fonctionnalités disponibles dans cette région, veuillez consulter Régions et points de terminaison.</p>	19 avril 2023

[GuardDuty ajout de 3 nouveaux types de résultats EC2](#)

5 avril 2023

GuardDuty introduit de nouveaux types de recherche pour détecter l'utilisation de résolveurs DNS externes et de technologies DNS cryptées. Pour plus d'informations sur les Régions AWS domaines dans lesquels ces types de recherche sont pris en charge, consultez [Régions et points de terminaison](#).

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

[GuardDuty annonce la surveillance du temps d'exécution d'EKS dans EKS Protection](#)

30 mars 2023

La surveillance du temps d'exécution EKS intégrée à EKS Protection permet de détecter les menaces d'exécution pour vos clusters Amazon EKS dans votre AWS environnement. Il utilise un agent de module complémentaire Amazon EKS (aws-guardduty-agent) qui collecte les [événements d'exécution](#) de vos charges de travail EKS. Après avoir GuardDuty reçu ces événements d'exécution, il les surveille et les analyse afin d'identifier les menaces de sécurité suspectes potentielles. Pour plus d'informations, veuillez consulter les sections [Détails du résultat](#) et [Types de résultat de la surveillance d'exécution EKS](#).

[GuardDuty ajoute une nouvelle fonctionnalité — autoEnableOrganizationMembers](#)

Amazon GuardDuty ajoute une nouvelle option de configuration d'organisation qui permet aux GuardDuty administrateurs d'auditer et de faire appliquer (si nécessaire) les comptes des administrateurs. Cette option GuardDuty est activée pour ALL les membres de leur organisation. Il est recommandé d'utiliser `autoEnableOrganizationMembers` au lieu de `autoEnable`. `autoEnable` est obsolète, mais toujours pris en charge. Les API suivantes sont concernées par cette nouvelle fonctionnalité :

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[La fonctionnalité de protection RDS d'Amazon GuardDuty est désormais disponible pour tous](#)

GuardDuty RDS Protection surveille et établit le profil de l'activité de connexion RDS afin d'identifier les comportements de connexion suspects sur vos instances de base de données Amazon Aurora. Pour plus d'informations sur les Régions AWS qui prennent en charge la protection RDS, veuillez consulter [Régions et points de terminaison](#).

16 mars 2023

[GuardDuty annonce l'activation de la fonctionnalité](#)

Historiquement, l'API GuardDuty autorisait la configuration des fonctionnalités et des sources de données, mais désormais, tous les nouveaux types de GuardDuty protection seront configurés en tant que fonctionnalités et non en tant que sources de données. GuardDuty prend toujours en charge les sources de données via l'API mais n'ajoutera pas de nouvelle API. L'activation des fonctionnalités affecte le comportement des API utilisées pour activer GuardDuty ou le type de protection qu'elles contiennent GuardDuty. Si vous gérez vos GuardDuty comptes via une API, un SDK ou un modèle CFN, consultez les [modifications apportées à GuardDuty l'API en mars 2023](#).

16 mars 2023

[GuardDuty La protection contre les logiciels malveillants pour EC2 est désormais disponible dans la région Moyen-Orient \(EAU\)](#)

La fonctionnalité de protection contre les programmes malveillants pour EC2 GuardDuty est prise en charge dans la région du Moyen-Orient (Émirats arabes unis). Pour plus d'informations, consultez [Régions et points de terminaison](#).

13 mars 2023

[Amazon GuardDuty a mis à jour le Service-linked rôle \(SLR\)](#)

GuardDuty a ajouté les nouvelles autorisations suivantes pour prendre en charge la prochaine fonctionnalité de surveillance du GuardDuty temps d'exécution d'EKS.

8 mars 2023

- Utilisez les actions Amazon EKS pour gérer et récupérer des informations sur les clusters EKS, et gérer les modules complémentaires EKS sur des clusters EKS. Les actions EKS récupèrent également les informations relatives aux balises associées à GuardDuty.

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"ec2:DescribeVpcEndpointServices",  
"ec2:DescribeSecurityGroups"
```

[Amazon GuardDuty a mis à jour le Service-linked rôle \(SLR\)](#)

Le GuardDuty SLR a été mis à jour pour permettre la création d'une protection contre les programmes malveillants pour EC2 SLR une fois que la protection contre les programmes malveillants pour EC2 a été activée.

21 février 2023

[GuardDuty nécessite TLS v1.2 ou version ultérieure](#)

Pour communiquer avec les AWS ressources, GuardDuty nécessite et prend en charge le protocole TLS v1.2 ou version ultérieure. Pour plus d'informations, veuillez consulter [Protection des données](#) et [Sécurité de l'infrastructure](#).

14 février 2023

[GuardDuty est désormais disponible dans la région Asie-Pacifique \(Hyderabad\)](#)

La région Asie-Pacifique (Hyderabad) a été ajoutée à la liste des régions Régions AWS disponibles GuardDuty . Pour plus d'informations, consultez [Régions et points de terminais on](#).

14 février 2023

[Le guide de GuardDuty l'utilisateur Amazon est conforme aux meilleures pratiques en matière d'IAM](#)

Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).

10 février 2023

[GuardDuty est désormais disponible dans la région Europe \(Espagne\)](#)

L'Europe (Espagne) a été ajoutée à la liste Régions AWS des pays GuardDuty où elle est disponible. Pour plus d'informations, consultez [Régions et points de terminais on](#).

8 février 2023

[GuardDuty est désormais disponible dans la région Europe \(Zurich\)](#)

L'Europe (Zurich) a été ajoutée à la liste Régions AWS des GuardDuty destinations disponibles. Pour plus d'informations, consultez [Régions et points de terminais on.](#)

12 décembre 2022

[Version préliminaire d'une nouvelle fonctionnalité : GuardDuty RDS Protection](#)

GuardDuty RDS Protection surveille et établit le profil de l'activité de connexion RDS afin d'identifier les comportements de connexion suspects sur vos instances de base de données Amazon Aurora. Actuellement, elle est disponible pour une version préliminaire dans cinq Régions AWS. Pour plus d'informations, consultez [Régions et points de terminais on.](#)

30 novembre 2022

[GuardDuty est désormais disponible dans la région Moyen-Orient \(EAU\)](#)

Le Moyen-Orient (EAU) a été ajouté à la liste des pays Régions AWS où GuardDuty il est disponible. Pour plus d'informations, consultez [Régions et points de terminais on.](#)

6 octobre 2022

[Ajout de contenu pour une nouvelle fonctionnalité : GuardDuty Malware Protection for EC2](#)

GuardDuty Malware Protection for EC2 est une amélioration optionnelle d'Amazon GuardDuty. Tout en GuardDuty identifiant les ressources à risque, Malware Protection for EC2 détecte les malwares susceptibles d'être à l'origine de la compromission. Lorsque Malware Protection for EC2 est activée, chaque fois qu'un comportement suspect est GuardDuty détecté sur une instance Amazon EC2 ou qu'une charge de travail de conteneur indique la présence d'un logiciel malveillant GuardDuty, Malware Protection for EC2 lance une analyse sans agent sur les volumes EBS attachés aux charges de travail d'instance ou de conteneur EC2 concernées afin de détecter la présence de logiciels malveillants. Pour plus d'informations sur le fonctionnement de Malware Protection for EC2 et sur la configuration de cette fonctionnalité, consultez [GuardDuty Malware Protection for EC2](#).

- Pour plus d'informations sur les résultats de la protection contre les programmes

26 juillet 2022

s malveillants pour EC2,
consultez la section
[Recherche de détails](#).

- Pour plus d'informations sur la correction de l'instance EC2 compromise et d'un conteneur autonome, consultez la section Résolution des [problèmes de sécurité découverts](#) par GuardDuty
- Pour plus d'informations sur les CloudWatch journaux d'audit pour les analyses de programmes malveillants et les raisons pour lesquelles une ressource est ignorée lors d'une analyse de programmes malveillants, consultez la section [Comprendre CloudWatch les journaux et les raisons des sauts](#).
- Pour plus d'informations sur les détections de faux positifs, consultez la section [Signalement des faux positifs dans GuardDuty Malware Protection for EC2](#).

[Retrait d'un type de résultat](#)

[Exfiltration:S3/ObjectRead.Unusual](#) a été retiré.

5 juillet 2022

[Ajout de nouveaux types de recherche S3 qui identifient les comportements anormaux à l'aide GuardDuty du modèle d'apprentissage automatique \(ML\) de détection des anomalies.](#)

5 juillet 2022

Les nouveaux types de résultat S3 suivants ont été ajoutés. Ces types de résultat identifient si une demande d'API a invoqué une entité IAM de manière anormale. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Pour en savoir plus sur chacun de ces nouveaux résultats, veuillez consulter [Types de résultat S3](#) (langue française non garantie).

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[Ajout de contenu de protection GuardDuty EKS pour GuardDuty](#)

GuardDuty peut désormais générer des résultats pour vos ressources Amazon EKS grâce à la surveillance des journaux d'audit EKS. Pour savoir comment configurer cette fonctionnalité, consultez [EKS Protection sur Amazon GuardDuty](#). Pour obtenir une liste des résultats que GuardDuty vous pouvez générer pour les ressources Amazon EKS, consultez les résultats de [Kubernetes](#). De nouvelles directives de correction ont été ajoutées pour permettre de corriger ces résultats dans le [guide de correction des résultats Kubernetes](#).

25 janvier 2022

[Ajout d'un nouveau résultat](#)

Un nouveau résultat, UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS, a été ajouté. Ce résultat vous informe lorsqu'un AWS compte extérieur à votre AWS environnement accède aux informations d'identification de votre instance.

20 janvier 2022

[Mise à jour des types de résultat pour simplifier l'identification des problèmes liés à log4j](#)

Amazon GuardDuty a mis à jour les types de recherche suivants afin d'identifier et de hiérarchiser les problèmes liés à CVE-2021-44228 et CVE-2021-45046 :
Backdoor:EC2/C&CActivity.B ;
Backdoor:EC2/C&CActivity.B!
DNS ;Behavior:EC2/NetworkPortUnusual.

22 décembre 2021

[Modifications des résultats](#)

Remplacement de UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration par UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS Cette version améliorée du résultat apprend les emplacements habituels à partir desquels vos informations d'identification sont utilisées afin de réduire les résultats provenant du trafic acheminé via des réseaux sur site.
[UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)

7 septembre 2021

[Mise à jour vers GuardDuty SLR](#)

Le GuardDuty SLR a été mis à jour avec de nouvelles actions visant à améliorer la précision de la recherche.

3 août 2021

[Informations de source de données ajoutées pour chaque type de résultat.](#)

Les descriptions de recherche contiennent désormais des informations sur les sources de données GuardDuty utilisées pour générer cette recherche.

10 mai 2021

[Retrait de 13 types de résultat.](#)

13 résultats ont été retirés pour être remplacés par de nouveaux AnomalousBehavior résultats. [Persistence:IAMUser/NetworkPermissions](#), [Persistence:IAMUser/ResourcePermissions](#), [Persistence:IAMUser/UserPermissions](#), [PrivilegeEscalation:IAMUser/AdministrativePermissions](#), [Recon:IAMUser/NetworkPermissions](#), [Recon:IAMUser/ResourcePermissions](#), [Recon:IAMUser/UserPermissions](#), [ResourceConsumption:IAMUser/ComputeResources](#), [Stealth:IAMUser/LoggingConfigurationModified](#), [Discovery:S3/BucketEnumeration.Unusual](#), [Impact:S3/ObjectDelete.Unusual](#), [Impact:S3/PermissionsModification.Unusual](#), et [UnauthorizedAccess:IAMUser/ConsoleLogin](#).

12 mars 2021

[Ajout de 8 nouveaux types de résultat pour les comportements anormaux.](#)

Ajout de 8 nouveaux types de résultat IAMUser basés sur un comportement anormal pour les principaux IAM. [CredentialAccess:IAMUser/AnomalousBehavior](#), [DefenseEvasion:IAMUser/AnomalousBehavior](#), [Discovery:IAMUser/AnomalousBehavior](#), [Exfiltration:IAMUser/AnomalousBehaviorImpact:IAMUser/AnomalousBehavior](#), [InitialAccess:IAMUser/AnomalousBehavior](#), [Persistence:IAMUser/AnomalousBehavior](#), [PrivilegeEscalation:IAMUser/AnomalousBehavior](#).

12 mars 2021

[Ajout de résultats EC2 basés sur la réputation du domaine.](#)

Ajout de 4 nouveaux types de résultat Impact basés sur la réputation du domaine. [Impact:EC2/AbusedDomainRequest.Reputation](#), [Impact:EC2/BitcoinDomainRequest.Reputation](#), [Impact:EC2/MaliciousDomainRequest.Reputation](#). Un nouveau résultat EC2 a également été ajouté pour C&CActivity. [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

27 janvier 2021

Ajout de 4 nouveaux types de résultat.	Ajout de 3 nouveaux résultats S3 MaliciousIPCaller. Discovery:S3/MaliciousIPCallerExfiltration:S3/MaliciousIPCaller , Impact:S3/MaliciousIPCaller . Un nouveau résultat EC2 a également été ajouté pour C&CActivity. Backdoor:EC2/C&CActivity.B	21 décembre 2020
Suppression du type de résultat UnauthorizedAccess:EC2/TorIPCaller.	Le type de UnauthorizedAccess:EC2/TorIPCaller recherche est désormais retiré de GuardDuty. En savoir plus.	1er octobre 2020
Ajout du type de résultat Impact:EC2/WinRmBruteForce.	Ajout d'un nouveau résultat Impact, Impact:EC2/WinRmBruteForce. En savoir plus.	17 septembre 2020
Ajout du type de résultat Impact:EC2/PortSweep.	Ajout d'un nouveau résultat Impact, Impact:EC2/PortSweep. En savoir plus.	17 septembre 2020
GuardDuty est désormais disponible dans les régions Afrique (Le Cap) et Europe (Milan).	L'Afrique (Le Cap) et l'Europe (Milan) ont été ajoutées à la liste des AWS régions disponibles. GuardDuty En savoir plus	31 juillet 2020

[Ajout de nouveaux détails d'utilisation pour le suivi des GuardDuty coûts.](#)

Vous pouvez désormais utiliser de nouvelles mesures pour interroger les données relatives aux coûts GuardDuty d'utilisation de votre compte et des comptes que vous gérez. Un nouvel aperçu des coûts d'utilisation est disponible dans la console à l'adresse <https://console.aws.amazon.com/guardduty/>. Des informations plus détaillées sont accessibles via l'API.

31 juillet 2020

[Ajout de contenu couvrant la protection S3 via la surveillance des événements de données S3 dans GuardDuty.](#)

GuardDuty S3 Protection est désormais disponible via la surveillance des événements du plan de données S3 en tant que nouvelle source de données. Cette fonctionnalité sera automatiquement activée pour les nouveaux comptes. Si vous l'utilisez déjà, GuardDuty vous pouvez activer la nouvelle source de données pour vous-même ou pour vos comptes membres.

31 juillet 2020

[Ajout de 14 nouveaux résultats S3.](#)

14 nouveaux types de résultats S3 ont été ajoutés pour les sources du plan de contrôle et du plan de données S3.

31 juillet 2020

[Ajout d'une prise en charge supplémentaire pour les résultats S3 et modification de 2 noms de types de résultat existants.](#)

GuardDuty les résultats incluent désormais plus de détails sur les résultats impliquant des compartiments S3. Les types de résultat existants qui étaient liés à l'activité S3 ont été renommés : Policy:IAMUser/S3BlockPublicAccessDisabled a été modifié en Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled a été modifié en Stealth:S3/ServerAccessLoggingDisabled.

28 mai 2020

[Du contenu a été ajouté pour AWS Organizations l'intégration.](#)

GuardDuty s'intègre désormais aux administrateurs AWS Organizations délégués pour vous permettre de gérer les GuardDuty comptes au sein de votre organisation. Lorsque vous définissez un administrateur délégué comme compte d'GuardDuty administrateur, vous pouvez automatiquement autoriser tous GuardDuty les membres de l'organisation à être gérés par le compte d'administrateur délégué. Vous pouvez également l'activer automatiquement GuardDuty dans les nouveaux comptes AWS Organizations membres. [En savoir plus.](#)

20 avril 2020

[Ajout de contenu pour la fonctionnalité d'exportation des résultats.](#)

Ajout d'un contenu qui décrit la fonctionnalité d'exportation des résultats de GuardDuty.

14 novembre 2019

[Ajout du type de résultat UnauthorizedAccess:EC2/MetadataDNSRebind.](#)

Ajout d'un nouveau résultat Unauthorized, UnauthorizedAccess:EC2/MetadataDNSRebind. [En savoir plus.](#)

10 octobre 2019

[Ajout du type de résultat Stealth:IAMUser/S3ServerAccessLoggingDisabled.](#)

Ajout d'un nouveau résultat Stealth, Stealth:IAMUser/S3ServerAccessLoggingDisabled. [En savoir plus.](#)

10 octobre 2019

Ajout du type de résultat Policy:IAMUser/S3BlockPublicAccessDisabled.	Ajout d'un nouveau résultat Policy, Policy:IAMUser/S3BlockPublicAccessDisabled. En savoir plus.	10 octobre 2019
Suppression du type de résultat Backdoor:EC2/XORDDOS.	Le type de Backdoor:EC2/XORDDOS recherche est désormais retiré de GuardDuty. En savoir plus	12 juin 2019
Ajout du type de résultat PrivilegeEscalation.	Le type de résultat Privilege Escalation détecte lorsque les utilisateurs tentent d'attribuer des privilèges transférés plus permissifs à leurs comptes. En savoir plus	14 mai 2019
GuardDuty est désormais disponible dans la région Europe (Stockholm).	L'Europe (Stockholm) a été ajoutée à la liste des AWS régions disponibles. GuardDuty En savoir plus	9 mai 2019
Ajout d'un nouveau type de résultat, Recon:EC2/PortProbeEMRUnprotectedPort.	Ce résultat vous indique qu'un port EMR-related sensible d'une instance EC2 n'est pas bloqué et qu'il fait l'objet d'une enquête active. En savoir plus	8 mai 2019
Ajout de 5 nouveaux types de résultat qui détectent si vos instances EC2 sont susceptibles d'être utilisées pour les attaques Denial of Service (DoS).	Ces résultats vous informent des instances EC2 dans votre environnement qui se comportent d'une manière pouvant indiquer qu'elles sont utilisées pour réaliser des attaques Denial of Service (DoS) En savoir plus	8 mars 2019

[Ajout d'un nouveau type de résultat : Policy:IAMUser/RootCredentialUsage](#)

Policy:IAMUser/RootCredentialUsageLe type de recherche vous indique que les informations de connexion de votre utilisateur root Compte AWS sont utilisées pour envoyer des demandes programmatiques aux AWS services. [En savoir plus](#)

24 janvier 2019

[Le type de résultat UnauthorizedAccess:IAMUser/UnusualASNCaller a été retiré](#)

Le type de résultat UnauthorizedAccess:IAMUser/UnusualASNCaller a été retiré. Vous serez désormais informé des activités invoquées depuis des réseaux inhabituels via d'autres types de GuardDuty recherche actifs. Le type de résultat généré sera basé sur la catégorie de l'API qui a été invoquée depuis un réseau inhabituel. [En savoir plus](#)

21 décembre 2018

[Ajout de deux nouveaux types de résultat : PenTest:IAMUser/ParrotLinux et PenTest:IAMUser/PentooLinux](#)

Le type de résultat PenTest:IAMUser/ParrotLinux vous informe qu'un ordinateur exécutant Parrot Security Linux effectue des appels d'API en utilisant les informations d'identification qui appartiennent à votre compte AWS . Le type de résultat PenTest:IAMUser/PentooLinux vous informe qu'une machine exécutant Pentoo Linux effectue des appels d'API en utilisant les informations d'identification qui appartiennent à votre compte AWS . [En savoir plus](#)

21 décembre 2018

[Ajout de la prise en charge de la rubrique Amazon GuardDuty Annonces \(SNS\)](#)

Vous pouvez désormais vous abonner à la rubrique SNS des GuardDuty annonces pour recevoir des notifications concernant les nouveaux types de résultats, les mises à jour des types de résultats existants et les autres modifications apportées aux fonctionnalités. Les notifications sont proposées dans tous les formats pris en charge par Amazon SNS. [En savoir plus](#)

21 novembre 2018

[Ajout de deux nouveaux types de résultat : UnauthorizedAccess:EC2/TorClient et UnauthorizedAccess:EC2/TorRelay](#)

UnauthorizedAccess:EC2/TorClient type de recherche vous indique qu'une instance EC2 de votre AWS environnement établit des connexions à un nœud Tor Guard ou Authority. UnauthorizedAccess:EC2/TorRelayfinding type vous indique qu'une instance EC2 de votre AWS environnement établit des connexions à un réseau Tor d'une manière qui suggère qu'elle agit comme un relais Tor. [En savoir plus](#)

16 novembre 2018

[Ajout d'un nouveau type de résultat : CryptoCurrency:EC2/BitcoinTool.B](#)

Ce résultat vous indique qu'une instance EC2 de votre AWS environnement interroge un nom de domaine associé à Bitcoin ou à une autre activité liée aux cryptomonnaies. [En savoir plus](#)

9 novembre 2018

[Ajout de la prise en charge de la mise à jour de la fréquence des notifications envoyées à CloudWatch Events](#)

Vous pouvez désormais mettre à jour la fréquence des notifications envoyées à CloudWatch Events pour les occurrences ultérieures de résultats existants. Les valeurs possibles sont 15 minutes, 1 heure ou, par défaut, 6 heures. [En savoir plus](#)

9 octobre 2018

Prise en charge de régions supplémentaires	Ajout du support régional pour AWS GovCloud (US-West) En savoir plus	25 juillet 2018
Ajout du support pour CloudFormation StackSets dans GuardDuty	Vous pouvez utiliser le GuardDuty modèle Enable Amazon pour activer GuardDuty simultanément plusieurs comptes. En savoir plus	25 juin 2018
Ajout de la prise en charge des GuardDuty règles d'archivage automatique	Les clients peuvent désormais créer des règles fines d'archivage automatique pour la suppression de résultats. Pour les résultats correspondant à une règle d'archivage automatique, marquez-les GuardDuty automatiquement comme archivés. Cela permet aux clients de poursuivre les réglages GuardDuty pour ne conserver que les résultats pertinents dans le tableau des résultats actuel. En savoir plus	4 mai 2018
GuardDuty est disponible dans la région Europe (Paris)	GuardDuty est désormais disponible en Europe (Paris), ce qui vous permet d'étendre la surveillance continue de la sécurité et la détection des menaces dans cette région. En savoir plus	29 mars 2018

[La création de comptes d'GuardDuty administrateur et de comptes de membre via CloudFormation est désormais prise en charge.](#)

Pour plus d'informations, consultez [AWS::GuardDuty::master](#) et [AWS::GuardDuty::member](#).

6 mars 2018

[Ajout de neuf nouvelles détections CloudTrail-based d'anomalies.](#)

Ces nouveaux types de recherche sont automatiquement activés GuardDuty dans toutes les régions prises en charge. [En savoir plus](#)

28 février 2018

[Ajout de trois nouvelles détections de renseignements sur les menaces \(types de recherche\).](#)

Ces nouveaux types de recherche sont automatiquement activés GuardDuty dans toutes les régions prises en charge. [En savoir plus](#)

5 février 2018

[Augmentation des limites pour les comptes des GuardDuty membres.](#)

Avec cette version, vous pouvez ajouter jusqu'à 1 000 comptes GuardDuty membres par AWS compte (compte GuardDuty administrateur). [En savoir plus](#)

25 janvier 2018

[Modifications apportées au téléchargement et gestion ultérieure des listes d'adresses IP fiables et des listes de menaces pour les comptes d'GuardDuty administrateur et les comptes de membres.](#)

Avec cette version, les utilisateurs de GuardDuty comptes d'administrateur peuvent télécharger et gérer des listes d'adresses IP fiables et des listes de menaces. Les utilisateurs des GuardDuty comptes membres ne peuvent pas télécharger et gérer des listes. Les listes d'adresses IP fiables et les listes de menaces téléchargées par le compte administrateur sont imposées aux GuardDuty fonctionnalités de ses comptes membres. [En savoir plus](#)

25 janvier 2018

Mises à jour antérieures

Modifier	Description	Date
Publication initiale	Publication initiale du guide de GuardDuty l'utilisateur Amazon.	28 novembre 2017

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.