



Guida per GuardDuty l'utente di Amazon

Amazon GuardDuty



Amazon GuardDuty: Guida per GuardDuty l'utente di Amazon

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è GuardDuty?	1
Caratteristiche di GuardDuty	2
Conformità PCI DSS	6
Prezzi in GuardDuty	7
Utilizzo GuardDuty della prova gratuita di 30 giorni	7
Utilizzo di Malware Protection for S3 con piano gratuito di 12 mesi	9
Accedendo GuardDuty	9
Concetti e termini chiave	11
Nozioni di base	16
Prima di iniziare	16
Passaggio 1: abilitare Amazon GuardDuty	18
Fase 2: generare esiti di esempio ed esplorare le operazioni di base	20
Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3	22
Passaggio 4: configura la GuardDuty ricerca di avvisi tramite SNS	27
Fasi successive	30
Origini dati fondamentali	31
AWS CloudTrail eventi di gestione	31
Come GuardDuty gestisce gli eventi AWS CloudTrail globali	32
Log di flusso VPC	33
Registri delle query DNS di Route53 Resolver	34
Rilevamento esteso delle minacce	35
Esempi di scenari di minaccia relativi alla sequenza di attacco	35
Come funziona Extended Threat Detection	36
Attivazione di piani di protezione per massimizzare il rilevamento delle minacce	37
Rilevamento delle sequenze di attacco nei cluster Amazon EKS	38
Rilevamento delle sequenze di attacco nei bucket Amazon S3	39
Rilevamento delle sequenze di attacco nei cluster Amazon ECS	40
Rilevamento delle sequenze di attacco nei gruppi di istanze Amazon EC2	40
Rilevamento esteso delle minacce nella console GuardDuty	41
Comprensione e gestione dei risultati della sequenza di attacco	42
Risorse aggiuntive	42
Protezione EKS	43
Registri di controllo EKS in EKS Protection	44
Abilitazione della protezione EKS in ambienti con più account	44

Attivazione di EKS Protection per un account autonomo	52
Protezione S3	54
AWS CloudTrail eventi relativi ai dati per S3	55
In che modo GuardDuty utilizza gli eventi CloudTrail relativi ai dati per S3	55
GuardDuty utilizzo di eventi CloudTrail relativi ai dati per S3 per le sequenze di attacco	56
Abilitazione della protezione S3 in ambienti con più account	56
Attivazione di S3 Protection per un account autonomo	63
Monitoraggio del runtime	65
Come funziona	66
Con i cluster Amazon EKS	67
Con istanze Amazon EC2	72
Con Fargate (solo Amazon ECS)	75
Dopo aver abilitato il monitoraggio del runtime	78
Prova gratuita di 30 giorni	79
Sto usando il periodo di GuardDuty prova o non ho mai abilitato EKS Runtime Monitoring	79
Ho abilitato EKS Runtime Monitoring prima del lancio di Runtime Monitoring	80
Prerequisiti	81
Per l'istanza EC2	81
Per il cluster Fargate (solo ECS)	87
Per il cluster EKS	93
Abilitazione del monitoraggio del runtime	97
Abilitazione del monitoraggio del runtime per ambienti con più account	98
Abilitare il monitoraggio del runtime per un account autonomo	102
Gestione degli agenti GuardDuty di sicurezza	103
Agente automatizzato sulla risorsa Amazon EC2	103
Gestione manuale degli agenti per le risorse Amazon EC2	116
Agente automatizzato su Fargate (solo Amazon ECS)	132
Agente automatizzato sulla risorsa Amazon EKS	168
Gestione manuale degli agenti per il cluster Amazon EKS	206
Configura i parametri aggiuntivi EKS	215
Convalida della configurazione degli endpoint VPC	218
Problemi di copertura del runtime e risoluzione dei problemi	220
Copertura e risoluzione dei problemi per le risorse Amazon EC2	220
Copertura e risoluzione dei problemi per i cluster Amazon ECS	237
Copertura e risoluzione dei problemi per i cluster Amazon EKS	252
Configurazione del monitoraggio della CPU e della memoria	269

Utilizzo di un VPC condiviso	270
Come funziona	271
Prerequisiti	273
Utilizzo di IaC con agenti automatizzati	274
Panoramica del grafico sulla dipendenza delle risorse IaC	274
Problema comune: eliminazione di risorse in IaC	275
Tipi di eventi di runtime raccolti	276
Eventi di processo	276
Eventi del container	278
AWS Fargate (solo Amazon ECS) eventi relativi alle attività	279
Eventi pod di Kubernetes	280
Eventi del Domain Name System (DNS)	280
Eventi aperti	281
Evento modulo di caricamento	281
Eventi mprotect	282
Eventi di montaggio	282
Eventi di collegamento	283
Eventi collegamento simbolico	283
Eventi dup	283
Evento mappa di memoria	284
Eventi socket	284
Connetti eventi	285
Eventi VM Readv processo	286
Eventi VM Writev processo	286
Eventi Process Trace (Ptrace)	287
Associa eventi	288
Ascolta gli eventi	288
Rinomina gli eventi	289
Imposta gli eventi relativi all'ID utente (UID)	289
Eventi Chmod	290
Agente di hosting del repository Amazon ECR GuardDuty	290
Repo ECR per EKS v1.12.1 - 1.8.1 (eks.build.2)	290
Repo ECR per la versione EKS 1.8.1.eks.build.1	295
Repository ECR per agente di sicurezza su (solo AWS Fargate Amazon ECS)	298
Agenti di sicurezza sullo stesso host	302
Panoramica di	302

Impatto	303
Come GuardDuty gestisce più agenti	303
Monitoraggio del runtime EKS	304
Configurazione di EKS Runtime Monitoring per ambienti con più account (API)	304
Configurazione di EKS Runtime Monitoring per un account autonomo (API)	345
Migrazione da EKS Runtime Monitoring a Runtime Monitoring	352
GuardDuty versioni di rilascio di Security Agent	356
Risorse aggiuntive: fasi successive	389
Disabilitazione, disinstallazione e pulizia delle risorse	389
Disinstallazione manuale dell'agente di sicurezza per le risorse Amazon EC2	391
Pulizia delle risorse del Security Agent	393
Protezione da malware per EC2	395
Confronto tra la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta	396
In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware	399
Volumi EBS supportati	400
Modifica l'ID della chiave KMS predefinita	401
Configura la conservazione delle istantanee e la copertura delle scansioni EC2	402
Conservazione delle istantanee	403
Opzioni di scansione con tag definiti dall'utente	404
Tag GuardDutyExcluded globale	408
GuardDuty-scansione antimalware avviata	408
Prova gratuita di 30 giorni	410
Abilitazione della scansione GuardDuty antimalware avviata in ambienti con più account	411
Attivazione della scansione antimalware GuardDuty avviata per un account autonomo	422
Risultati che richiamano la scansione GuardDuty antimalware avviata	423
Scansione antimalware on demand	426
Come funziona la scansione antimalware on demand	427
Avvio della scansione antimalware su richiesta	428
Nuova scansione dell'istanza Amazon EC2 precedentemente scansionata	430
Monitoraggio dello stato e del risultato delle scansioni malware	431
GuardDuty account di servizio	433
Quote nella protezione da malware per EC2	436
Protezione da malware per S3	441
Prezzi e costi di utilizzo	443
Revisione dei costi di utilizzo	444

Come funziona	444
Panoramica di	445
Autorizzazioni del ruolo IAM	445
Etichettatura opzionale degli oggetti in base al risultato della scansione	445
Procedura dopo aver abilitato Malware Protection for S3 per un bucket	446
Funzionalità di protezione da malware per S3	448
(Facoltativo) Inizia a usare Malware Protection solo per S3 (console)	449
Configurazione della protezione da malware per S3 per il tuo bucket	450
Attivazione del rilevamento delle minacce da parte di Malware Protection for S3 per il tuo bucket	451
Autorizzazioni del ruolo IAM	458
Risoluzione dell'errore relativo alle autorizzazioni dei ruoli IAM	463
Passaggi dopo l'attivazione di Malware Protection for S3	464
Scansione antimalware S3 su richiesta	465
Prerequisiti	466
Avvia una scansione antimalware su richiesta	466
Utilizzo del controllo degli accessi basato su tag (TBAC)	467
Aggiungere TBAC alla risorsa bucket S3	468
Visualizza e comprendi lo stato del bucket protetto	470
Monitoraggio delle scansioni degli oggetti S3	471
Potenziale stato di scansione dell'oggetto S3 e stato dei risultati	472
Usare Amazon EventBridge	473
Utilizzo dei tag degli oggetti S3	483
Utilizzo di CloudWatch allarmi e metriche	484
Risoluzione dei problemi	487
Risoluzione dei problemi relativi allo stato del piano di protezione contro	487
Risoluzione dei problemi relativi alla scansione antimalware su richiesta	491
Modifica del piano di protezione da malware per un bucket protetto	491
Disattivazione di Malware Protection for S3 per un bucket protetto	493
Supportabilità delle funzionalità di Amazon S3	495
Protezione da malware per le quote S3	503
Protezione da malware per il AWS backup	505
Panoramica di	505
Come funziona	508
Panoramica di	505
Ruolo IAM richiesto per la scansione	509

Revisione dello stato e dei risultati della scansione delle risorse	509
Revisione dei risultati generati	510
Autorizzazioni IAM Role	511
Ruolo del cliente fornito per la scansione del malware	511
Dettagli sulle autorizzazioni	511
Garantire il ruolo	512
In che modo GuardDuty Malware Protection utilizza le sovvenzioni in KMS AWS	512
GuardDuty Contesto di crittografia della protezione da malware	513
Autorizzazioni e politica di fiducia per il ruolo	514
Inizia in modo indipendente	518
Passaggi per iniziare a usare Malware Protection for Backup	518
Avvio di scansioni su richiesta	519
Console	519
API/CLI	520
Monitoraggio dello stato e del risultato delle scansioni malware	520
Protezione da malware per quote di Backup	528
Protezione RDS	532
Database supportati	533
Attività di accesso RDS	534
Abilitazione della protezione RDS in ambienti con più account	535
Attivazione della protezione RDS per un account autonomo	542
Risoluzione dei problemi di monitoraggio di RDS Protection	543
Archiviazione RDS completa	543
Versioni non supportate sul database primario per RDS per PostgreSQL	544
Ulteriori considerazioni sulla sicurezza	544
Protezione Lambda	545
Monitoraggio delle attività di rete Lambda	546
Abilitazione della protezione Lambda in ambienti con più account	546
Attivazione di Lambda Protection per un account autonomo	553
Protezione dei carichi di lavoro di intelligenza artificiale	555
Account multipli in GuardDuty	556
Relazioni tra account amministratore e account membro	556
Gestione degli account con AWS Organizations	561
Considerazioni e raccomandazioni	562
Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty	564
Designazione di un account amministratore delegato GuardDuty	565

Impostazione delle preferenze di attivazione automatica dell'organizzazione	567
Aggiungere membri all'organizzazione	571
(Facoltativo) Abilita i piani di protezione per gli account dei membri esistenti	574
Gestione continua degli account dei membri all'interno GuardDuty	574
Sospensione GuardDuty per l'account di un membro	575
Dissociazione (rimozione) dell'account membro dall'account amministratore	577
Eliminazione degli account dei membri dall'organizzazione GuardDuty	579
Modifica dell' GuardDuty account amministratore delegato	580
Gestione degli account tramite invito	583
Aggiungere account su invito	584
Consolidamento degli account degli amministratori in un'unica organizzazione	589
GuardDuty considerazioni sull'opzione Esporta CSV negli account	591
Tipi di esiti	593
Tipi di esiti EC2	593
Backdoor:EC2/C&CAActivity.B	595
Backdoor:EC2/C&CAActivity.B!DNS	596
Backdoor:EC2/DenialOfService.Dns	597
Backdoor:EC2/DenialOfService.Tcp	598
Backdoor:EC2/DenialOfService.Udp	598
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	599
Backdoor:EC2/DenialOfService.UnusualProtocol	600
Backdoor:EC2/Spambot	600
Behavior:EC2/NetworkPortUnusual	601
Behavior:EC2/TrafficVolumeUnusual	601
CryptoCurrency:EC2/BitcoinTool.B	602
CryptoCurrency:EC2/BitcoinTool.B!DNS	602
DefenseEvasion:EC2/UnusualDNSResolver	603
DefenseEvasion:EC2/UnusualDoHActivity	604
DefenseEvasion:EC2/UnusualDoTActivity	604
Impact:EC2/AbusedDomainRequest.Reputation	605
Impact:EC2/BitcoinDomainRequest.Reputation	605
Impact:EC2/MaliciousDomainRequest.Reputation	606
Impact:EC2/MaliciousDomainRequest.Custom	607
Impact:EC2/PortSweep	607
Impact:EC2/SuspiciousDomainRequest.Reputation	608
Impact:EC2/WinRMBruteForce	608

Recon:EC2/PortProbeEMRUnprotectedPort	609
Recon:EC2/PortProbeUnprotectedPort	610
Recon:EC2/Portscan	611
Trojan:EC2/BlackholeTraffic	611
Trojan:EC2/BlackholeTraffic!DNS	612
Trojan:EC2/DGADomainRequest.B	612
Trojan:EC2/DGADomainRequest.C!DNS	613
Trojan:EC2/DNSDataExfiltration	614
Trojan:EC2/DriveBySourceTraffic!DNS	615
Trojan:EC2/DropPoint	615
Trojan:EC2/DropPoint!DNS	616
Trojan:EC2/PhishingDomainRequest!DNS	616
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	617
UnauthorizedAccess:EC2/MetadataDNSRebind	617
UnauthorizedAccess:EC2/RDPBruteForce	618
UnauthorizedAccess:EC2/SSHBruteForce	619
UnauthorizedAccess:EC2/TorClient	620
UnauthorizedAccess:EC2/TorRelay	621
Tipi di esiti IAM	621
CredentialAccess:IAMUser/AnomalousBehavior	622
CredentialAccess:IAMUser/CompromisedCredentials	623
DefenseEvasion:IAMUser/AnomalousBehavior	624
DefenseEvasion:IAMUser/BedrockLoggingDisabled	625
Discovery:IAMUser/AnomalousBehavior	625
Exfiltration:IAMUser/AnomalousBehavior	626
Impact:IAMUser/AnomalousBehavior	627
InitialAccess:IAMUser/AnomalousBehavior	627
PenTest:IAMUser/KaliLinux	628
PenTest:IAMUser/ParrotLinux	629
PenTest:IAMUser/PentooLinux	629
Persistence:IAMUser/AnomalousBehavior	630
Policy:IAMUser/RootCredentialUsage	630
Policy:IAMUser/ShortTermRootCredentialUsage	631
PrivilegeEscalation:IAMUser/AnomalousBehavior	632
Recon:IAMUser/MaliciousIPCaller	632
Recon:IAMUser/MaliciousIPCaller.Custom	633

Recon:IAMUser/TorIPCaller	633
Stealth:IAMUser/CloudTrailLoggingDisabled	634
Stealth:IAMUser/PasswordPolicyChange	634
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	635
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	636
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	638
UnauthorizedAccess:IAMUser/MaliciousIPCaller	639
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	640
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	640
UnauthorizedAccess:IAMUser/TorIPCaller	641
tipi di ricerca delle sequenze di attacco	642
AttackSequence:EKS/CompromisedCluster	642
AttackSequence:ECS/CompromisedCluster	643
AttackSequence:EC2/CompromisedInstanceGroup	644
AttackSequence:IAM/CompromisedCredentials	645
AttackSequence:S3/CompromisedData	646
Tipi di risultati di protezione S3	647
Discovery:S3/AnomalousBehavior	648
Discovery:S3/MaliciousIPCaller	649
Discovery:S3/MaliciousIPCaller.Custom	649
Discovery:S3/TorIPCaller	650
Exfiltration:S3/AnomalousBehavior	650
Exfiltration:S3/MaliciousIPCaller	651
Impact:S3/AnomalousBehavior.Delete	652
Impact:S3/AnomalousBehavior.Permission	653
Impact:S3/AnomalousBehavior.Write	653
Impact:S3/MaliciousIPCaller	654
PenTest:S3/KaliLinux	655
PenTest:S3/ParrotLinux	655
PenTest:S3/Pentoolinux	656
Policy:S3/AccountBlockPublicAccessDisabled	656
Policy:S3/BucketAnonymousAccessGranted	657
Policy:S3/BucketBlockPublicAccessDisabled	658
Policy:S3/BucketPublicAccessGranted	659
Stealth:S3/ServerAccessLoggingDisabled	659
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	660

UnauthorizedAccess:S3/TorIPCaller	660
Tipi di risultati di protezione EKS	661
CredentialAccess:Kubernetes/MaliciousIPCaller	663
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	664
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	664
CredentialAccess:Kubernetes/TorIPCaller	665
DefenseEvasion:Kubernetes/MaliciousIPCaller	666
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	666
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	667
DefenseEvasion:Kubernetes/TorIPCaller	668
Discovery:Kubernetes/MaliciousIPCaller	668
Discovery:Kubernetes/MaliciousIPCaller.Custom	669
Discovery:Kubernetes/SuccessfulAnonymousAccess	670
Discovery:Kubernetes/TorIPCaller	671
Execution:Kubernetes/ExecInKubeSystemPod	671
Impact:Kubernetes/MaliciousIPCaller	672
Impact:Kubernetes/MaliciousIPCaller.Custom	673
Impact:Kubernetes/SuccessfulAnonymousAccess	673
Impact:Kubernetes/TorIPCaller	674
Persistence:Kubernetes/ContainerWithSensitiveMount	675
Persistence:Kubernetes/MaliciousIPCaller	675
Persistence:Kubernetes/MaliciousIPCaller.Custom	676
Persistence:Kubernetes/SuccessfulAnonymousAccess	677
Persistence:Kubernetes/TorIPCaller	677
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	678
Policy:Kubernetes/AnonymousAccessGranted	679
Policy:Kubernetes/ExposedDashboard	679
Policy:Kubernetes/KubeflowDashboardExposed	680
PrivilegeEscalation:Kubernetes/PrivilegedContainer	680
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	681
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	682
Execution:Kubernetes/AnomalousBehavior.ExecInPod	683
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!	
PrivilegedContainer	683
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!	
ContainerWithSensitiveMount	684

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	685
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	687
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	688
Tipi di risultati del monitoraggio del runtime	688
CryptoCurrency:Runtime/BitcoinTool.B	690
Backdoor:Runtime/C&CActivity.B	691
UnauthorizedAccess:Runtime/TorRelay	692
UnauthorizedAccess:Runtime/TorClient	693
Trojan:Runtime/BlackholeTraffic	694
Trojan:Runtime/DropPoint	694
CryptoCurrency:Runtime/BitcoinTool.B!DNS	695
Backdoor:Runtime/C&CActivity.B!DNS	696
Trojan:Runtime/BlackholeTraffic!DNS	697
Trojan:Runtime/DropPoint!DNS	698
Trojan:Runtime/DGADomainRequest.C!DNS	698
Trojan:Runtime/DriveBySourceTraffic!DNS	699
Trojan:Runtime/PhishingDomainRequest!DNS	700
Impact:Runtime/AbusedDomainRequest.Reputation	701
Impact:Runtime/BitcoinDomainRequest.Reputation	702
Impact:Runtime/MaliciousDomainRequest.Reputation	703
Impact:Runtime/SuspiciousDomainRequest.Reputation	703
UnauthorizedAccess:Runtime/MetadataDNSRebind	704
Execution:Runtime/NewBinaryExecuted	705
PrivilegeEscalation:Runtime/DockerSocketAccessed	706
PrivilegeEscalation:Runtime/RuncContainerEscape	707
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	708
DefenseEvasion:Runtime/ProcessInjection.Proc	709
DefenseEvasion:Runtime/ProcessInjection.Ptrace	710
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	710
Execution:Runtime/ReverseShell	711
DefenseEvasion:Runtime/FilelessExecution	712
Impact:Runtime/CryptoMinerExecuted	712
Execution:Runtime/NewLibraryLoaded	713
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	714
PrivilegeEscalation:Runtime/UserfaultfdUsage	714
Execution:Runtime/SuspiciousTool	715

Execution:Runtime/SuspiciousCommand	716
DefenseEvasion:Runtime/SuspiciousCommand	717
DefenseEvasion:Runtime/PtraceAntiDebugging	718
Execution:Runtime/MaliciousFileExecuted	718
Execution:Runtime/SuspiciousShellCreated	719
PrivilegeEscalation:Runtime/ElevationToRoot	720
Discovery:Runtime/SuspiciousCommand	721
Persistence:Runtime/SuspiciousCommand	722
PrivilegeEscalation:Runtime/SuspiciousCommand	723
DefenseEvasion:Runtime/KernelModuleLoaded	723
Protezione da malware per tipi di ricerca EC2	724
Execution:EC2/MaliciousFile	725
Execution:ECS/MaliciousFile	725
Execution:Kubernetes/MaliciousFile	726
Execution:Container/MaliciousFile	726
Execution:EC2/SuspiciousFile	727
Execution:ECS/SuspiciousFile	727
Execution:Kubernetes/SuspiciousFile	728
Execution:Container/SuspiciousFile	729
Protezione da malware per tipo di ricerca S3	729
Object:S3/MaliciousFile	730
Tipi di ricerca di Malware Protection for Backup	730
Execution:EC2/MaliciousFile!Snapshot	731
Execution:EC2/MaliciousFile!AMI	731
Execution:EC2/MaliciousFile!RecoveryPoint	732
Execution:S3/MaliciousFile!RecoveryPoint	732
Tipi di esiti della Protezione RDS	732
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	733
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	734
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	735
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	736
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	737
Discovery:RDS/MaliciousIPCaller	737
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	738
CredentialAccess:RDS/TorIPCaller.FailedLogin	738
Discovery:RDS/TorIPCaller	739

Tipi di esiti della Protezione Lambda	740
Backdoor:Lambda/C&CActivity.B	740
CryptoCurrency:Lambda/BitcoinTool.B	741
Trojan:Lambda/BlackholeTraffic	742
Trojan:Lambda/DropPoint	742
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	743
UnauthorizedAccess:Lambda/TorClient	743
UnauthorizedAccess:Lambda/TorRelay	744
Tipi di esiti ritirati	744
Exfiltration:S3/ObjectRead.Unusual	745
Impact:S3/PermissionsModification.Unusual	746
Impact:S3/ObjectDelete.Unusual	746
Discovery:S3/BucketEnumeration.Unusual	747
Persistence:IAMUser/NetworkPermissions	748
Persistence:IAMUser/ResourcePermissions	748
Persistence:IAMUser/UserPermissions	749
PrivilegeEscalation:IAMUser/AdministrativePermissions	750
Recon:IAMUser/NetworkPermissions	751
Recon:IAMUser/ResourcePermissions	752
Recon:IAMUser/UserPermissions	752
ResourceConsumption:IAMUser/ComputeResources	753
Stealth:IAMUser/LoggingConfigurationModified	754
UnauthorizedAccess:IAMUser/ConsoleLogin	755
UnauthorizedAccess:EC2/TorIPCaller	755
Backdoor:EC2/XORDDOS	756
Behavior:IAMUser/InstanceLaunchUnusual	756
CryptoCurrency:EC2/BitcoinTool.A	757
UnauthorizedAccess:IAMUser/UnusualASNCaller	757
GuardDuty ricerca dei tipi in base alle risorse potenzialmente interessate	757
GuardDuty tipi di ricerca attivi	758
Comprendere e generare risultati	781
GuardDuty formato di ricerca	782
Scopi delle minacce	783
GuardDuty motore di scansione per il rilevamento di malware	786
Risultati di esempio	787
Generazione di risultati di esempio tramite la GuardDuty console o l'API	788

GuardDuty Risultati dei test	789
Considerazioni	789
GuardDuty lo script del tester dei risultati può generare	791
Fase 1 - Prerequisiti	793
Fase 2 - Implementazione delle risorse AWS	794
Fase 3 - Esegui gli script dei tester	795
Fase 4 - Pulisci le risorse di test AWS	798
Risoluzione dei problemi comuni	798
Pagina dei risultati nella GuardDuty console	800
Navigazione nella pagina dei risultati	801
Livelli di gravità dei risultati	802
Gravità critica	803
Severità elevata	803
Gravità media	804
Bassa severità	804
Dettagli degli esiti	805
Panoramica degli esiti	806
Risorsa	807
Dettagli del reperimento della sequenza di attacco	813
Dettagli utente del database (DB) RDS	820
Dettagli sugli esiti del monitoraggio del runtime	820
Dettagli della scansione dei volumi EBS	822
Dettagli sulla ricerca di Malware Protection for EC2	823
Dettagli sugli esiti di Malware Protection per S3	824
Azione	825
Attore o destinazione	827
Dettagli sulla geolocalizzazione	828
Informazioni aggiuntive	828
Evidenza	829
Comportamento anomalo	829
GuardDuty ricerca dell'aggregazione	834
Gestione dei GuardDuty risultati	836
GuardDuty Pannello di controllo ri	837
Panoramica di	838
Esiti	839
Tipi di esiti più comuni	840

Esiti per gravità	840
Account con il maggior numero di esiti	841
Risorse con esiti	841
Esiti meno ricorrenti	842
Copertura dei piani di protezione	842
Filtraggio GuardDuty dei risultati	843
Creazione e salvataggio del set di filtri nella GuardDuty console	844
Creazione e salvataggio di set di filtri utilizzando GuardDuty API e CLI	846
Filtri di proprietà in GuardDuty	848
Regole di eliminazione	855
Utilizzo delle regole di soppressione con Extended Threat Detection	855
Casi d'uso comuni per le regole di eliminazione ed esempi	856
Creazione di regole di soppressione	859
Aggiornamento delle regole di soppressione	864
Eliminazione delle regole di soppressione	867
Elenchi di entità ed elenchi di indirizzi IP	868
Comprendere gli elenchi di entità e gli elenchi di indirizzi IP	868
Considerazioni importanti per gli elenchi GuardDuty	869
Formati di elenco	870
Comprensione degli stati degli elenchi	876
Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP	877
Aggiungere e attivare un elenco di entità o un elenco di IP	879
Aggiornamento di un elenco di entità o di indirizzi IP	885
Disattivazione dell'elenco di entità o dell'elenco di indirizzi IP	891
Eliminazione dell'elenco di entità o dell'elenco di indirizzi IP	893
Esportazione dei risultati generati su Amazon S3	896
Considerazioni	897
Fase 1 — Autorizzazioni necessarie per esportare i risultati	898
Fase 2: Allegare la policy alla chiave KMS	898
Fase 3: Allegare la policy al bucket Amazon S3	900
Fase 4 - Esportazione dei risultati in un bucket S3 (console)	904
Fase 5 — Frequenza di esportazione dei risultati	905
Elaborazione dei risultati con EventBridge	906
EventBridge frequenza di notifica in GuardDuty	907
Configurare un argomento e un endpoint di Amazon SNS	907
Utilizzo EventBridge con GuardDuty	909

Creazione di una regola EventBridge	911
EventBridge regola per ambienti con più account	917
Comprensione dei CloudWatch log e dei motivi per cui le risorse vengono ignorate	918
Controllo dei CloudWatch log in Malware Protection for EC2 GuardDuty	919
GuardDuty Protezione da malware per la conservazione dei log EC2	921
Motivi per cui una risorsa viene ignorata	921
Segnalazione di risultati di scansione EC2 malware falsi positivi	927
Segnalazione dei risultati di scansione degli oggetti S3 falsi positivi	928
Segnalazione di risultati falsi positivi della scansione del malware di Backup	929
Correzioni degli esiti	931
Correzione di un'istanza Amazon EC2 potenzialmente compromessa	931
Riparazione di un bucket S3 potenzialmente compromesso	933
Consigli basati su esigenze specifiche di accesso ai bucket S3	935
Riparazione di un oggetto S3 potenzialmente dannoso	936
Correzione di uno snapshot EBS potenzialmente compromesso	936
Correzione di un AMI EC2 potenzialmente compromesso	937
Riparazione di un punto di ripristino EC2 potenzialmente compromesso	938
Riparazione di un punto di ripristino S3 potenzialmente compromesso	939
Riparazione di un cluster ECS potenzialmente compromesso	940
Riparazione delle credenziali potenzialmente compromesse AWS	941
Riparazione di un contenitore autonomo potenzialmente compromesso	943
Correzione dei risultati della protezione EKS	944
Potenziati problemi di configurazione	945
Riparare gli utenti Kubernetes potenzialmente compromessi	945
Riparazione dei pod Kubernetes potenzialmente compromessi	948
Riparazione delle immagini dei container potenzialmente compromesse	949
Riparazione dei nodi Kubernetes potenzialmente compromessi	950
Riparazione degli esiti del monitoraggio del runtime	951
Correzione delle immagini del container compromesse	953
Ripristino di un database potenzialmente compromesso	953
Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti	954
Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti	955
Correzione di credenziali potenzialmente compromesse	956
Limita l'accesso alla rete	956

Correzione di una funzione Lambda potenzialmente compromessa	957
Monitoraggio dell'utilizzo e stima dei costi	958
Metriche CloudWatch di utilizzo di Amazon	958
Dettagli metrici	958
Protezione da malware per S3	961
Comprensione dell'utilizzo GuardDuty	962
GuardDuty Elaborazione degli eventi	962
GuardDuty Costi di elaborazione dei log di flusso VPC per le istanze monitorate da Runtime Monitoring GuardDuty	962
GuardDuty Stima dei costi	963
Clienti Security Hub	963
Nomi delle funzionalità per i piani di protezione nell'API	965
Passaggio dalle fonti di dati alle funzionalità	965
GuardDuty Modifiche all'API	965
Funzionalità rispetto alle fonti di dati	966
Capire come funzionano APIs le funzionalità	967
Incorporazione delle modifiche alle funzionalità in APIs	967
Caratteristica GuardDuty mappata	968
Sicurezza	971
Protezione dei dati	971
Crittografia dei dati a riposo	973
Crittografia dei dati in transito	973
Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio	973
Registrazione con CloudTrail	975
GuardDuty informazioni in CloudTrail	975
GuardDuty eventi del piano di controllo in CloudTrail	976
GuardDuty eventi relativi ai dati in CloudTrail	976
Esempio: voci dei file di registro GuardDuty	977
Identity and Access Management	980
Destinatari	981
Autenticazione con identità	981
Gestione dell'accesso tramite policy	982
Come GuardDuty funziona Amazon con IAM	984
Esempi di policy basate su identità	990
Uso di ruoli collegati ai servizi	999
AWS politiche gestite	1009

Risoluzione dei problemi	1024
Convalida della conformità	1026
Resilienza	1027
Sicurezza dell'infrastruttura	1027
Endpoint VPC (AWS PrivateLink)	1027
Considerazioni sugli endpoint GuardDuty VPC	1028
Creazione di un endpoint VPC di interfaccia per GuardDuty	1028
Creazione di una policy per gli endpoint VPC per GuardDuty	1028
Sottoreti condivise	1029
Integrazione con i servizi AWS di sicurezza	1030
Integrazione con GuardDuty AWS Security Hub CSPM	1030
Integrazione GuardDuty con Amazon Detective	1030
AWS Security Hub CSPM integrazione	1030
In che modo Amazon GuardDuty invia i risultati a AWS Security Hub CSPM	1031
Visualizzazione dei GuardDuty risultati in AWS Security Hub CSPM	1032
Abilitazione e configurazione dell'integrazione	1052
Utilizzo GuardDuty dei controlli in Security Hub CSPM	1052
Interruzione della pubblicazione dei risultati su Security Hub CSPM	1052
Integrazione con Amazon Detective	1052
Abilitazione dell'integrazione	1053
Passare ad Amazon Detective partendo da una scoperta GuardDuty	1053
Utilizzo dell'integrazione con un ambiente GuardDuty multi-account	1054
Sospensione o disabilitazione	1055
GuardDuty annunci	1057
Formato dei messaggi Amazon SNS	1063
GuardDuty quote	1069
Supporto per istanze gestite	1076
Risoluzione dei problemi	1077
Esportazione dei risultati su Amazon S3: errore di accesso	1077
Problemi relativi alla protezione da malware per EC2	1078
Manca l'autorizzazione AWS Organizations di gestione richiesta quando si abilita la scansione GuardDuty antimalware avviata	1078
All'avvio di una scansione antimalware on demand ricevo un messaggio di un errore che segnala la mancanza delle autorizzazioni richieste.	1078
Ricevo un iam:GetRole errore mentre lavoro con Malware Protection for EC2.	1078

Sono un account GuardDuty amministratore che deve abilitare la scansione antimalware	
GuardDuty avviata dall'utente ma non utilizza AWS Managed Policy: to manage.	
AmazonGuardDutyFullAccess GuardDuty	1079
Problemi di monitoraggio del runtime	1079
Problemi di copertura del runtime	1079
Risoluzione dell'errore di esaurimento della memoria	1079
Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto	1080
Altre questioni relative alla risoluzione dei problemi	1081
Regioni ed endpoint	1082
Disponibilità di funzionalità specifiche per ogni regione	1082
Operazioni e parametri legacy	1085
Cronologia dei documenti	1087
Aggiornamenti precedenti	1181
.....	mclxxxii

Che cos'è Amazon GuardDuty?

Amazon GuardDuty è un servizio di rilevamento delle minacce che monitora, analizza ed elabora continuamente le fonti di AWS dati e i log nel tuo ambiente. AWS GuardDuty utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, hash di file e modelli di machine learning (ML) per identificare attività sospette e potenzialmente dannose nel tuo ambiente. AWS L'elenco seguente fornisce una panoramica dei potenziali scenari di minaccia che GuardDuty possono aiutarti a rilevare:

- Credenziali compromesse ed esfiltrate AWS .
- Efiltrazione e distruzione dei dati che possono portare a un evento ransomware. Modelli insoliti di eventi di accesso nelle versioni del motore supportate dei database Amazon Aurora e Amazon RDS, che indicano un comportamento anomalo.
- Attività di cryptomining non autorizzate nelle istanze Amazon Elastic Compute Cloud (Amazon EC2) e nei carichi di lavoro dei container.
- Presenza di malware nelle istanze Amazon EC2 e nei carichi di lavoro dei container e file appena caricati nei bucket Amazon Simple Storage Service (Amazon S3).
- Eventi a livello di sistema operativo, di rete e di file che indicano un comportamento non autorizzato sui cluster Amazon Elastic Kubernetes Service (Amazon EKS), sulle attività di Amazon Elastic Container Service (Amazon ECS), sulle istanze Amazon EC2 e sui carichi di lavoro dei container AWS Fargate .

Il video seguente fornisce una panoramica di come ti aiuta a rilevare le minacce nel tuo ambiente.
GuardDuty AWS

[Che cos'è Amazon GuardDuty](#)

Indice

- [Caratteristiche di GuardDuty](#)
- [Conformità PCI DSS](#)
- [Prezzi in GuardDuty](#)
- [Accedendo GuardDuty](#)

Caratteristiche di GuardDuty

Ecco alcuni dei modi principali in cui Amazon GuardDuty può aiutarti a monitorare, rilevare e gestire le potenziali minacce nel tuo AWS ambiente.

Monitora continuamente fonti di dati e registri di eventi specifici

- Rilevamento delle minacce fondamentali: quando attivi GuardDuty in un Account AWS, avvia GuardDuty automaticamente l'acquisizione delle fonti di dati di base associate a quell'account. Queste fonti di dati includono eventi di AWS CloudTrail gestione, log di flusso VPC (da istanze Amazon EC2) e log DNS. Non è necessario abilitare nient'altro per iniziare ad analizzare ed

elaborare queste GuardDuty fonti di dati per generare i risultati di sicurezza associati. Per ulteriori informazioni, consulta [GuardDuty fonti di dati fondamentali](#).

- **Rilevamento esteso delle minacce:** questa funzionalità rileva attacchi in più fasi che coinvolgono fonti di dati fondamentali, più tipi di AWS risorse e tempi, all'interno di un unico Account AWS. Nel tuo account potrebbero verificarsi più eventi che, singolarmente, non rappresentano una minaccia evidente. Tuttavia, quando questi eventi vengono osservati in una sequenza indicativa di un'attività sospetta, la GuardDuty identifica come una sequenza di attacco. GuardDuty ti avvisa generando il tipo di ricerca della sequenza di attacco associata per fornire dettagli sulla sequenza di attacco osservata.

Senza costi aggiuntivi, Extended Threat Detection viene abilitato automaticamente per ciascuna di esse al Account AWS momento dell'attivazione. GuardDuty Questa funzionalità non richiede l'attivazione di alcun piano di protezione incentrato sui casi d'uso. Tuttavia, per aumentare l'ampiezza della sicurezza delle tue risorse Amazon S3 GuardDuty , ti consigliamo di abilitare S3 Protection nel tuo account. Questo aiuterà Extended Threat Detection a identificare gli attacchi in più fasi che potrebbero avere un impatto sulle tue risorse Amazon S3.

Per ulteriori informazioni su come funziona questa funzionalità e sugli scenari di minaccia coperti, consulta [GuardDuty Rilevamento esteso delle minacce](#)

- **Piani di GuardDuty protezione incentrati sui casi d'uso:** per una maggiore visibilità del rilevamento delle minacce nella sicurezza dell' AWS ambiente, GuardDuty offre piani di protezione dedicati che è possibile scegliere di abilitare. I piani di protezione consentono di monitorare i registri e gli eventi di altri servizi. AWS Queste fonti includono registri di controllo EKS, attività di accesso RDS, eventi dati CloudTrail in Amazon S3, volumi EBS, monitoraggio del runtime su Amazon EKS, Amazon EC2 e Amazon ECS-Fargate e registri delle attività di rete Lambda. GuardDuty[consolida queste fonti di log ed eventi sotto il termine - Caratteristiche](#). È possibile abilitare uno o più piani di protezione dedicati in un servizio supportato in qualsiasi Regione AWS momento. GuardDuty avvierà il monitoraggio, l'elaborazione e l'analisi delle attività in base al piano di protezione abilitato. Per ulteriori informazioni su ciascun piano di protezione e su come funziona, consulta il documento relativo al piano di protezione corrispondente.

Piano di protezione	Description
Protezione S3	Identifica i potenziali rischi per la sicurezza, come i tentativi di esfiltrazione e distruzione dei dati nei bucket Amazon S3.

Piano di protezione	Description
Protezione EKS	EKS Audit Log Monitoring analizza i log di controllo Kubernetes dai cluster Amazon EKS per attività potenzialmente sospette e dannose.
Monitoraggio del runtime	Monitora e analizza gli eventi a livello di sistema operativo su Amazon EKS, Amazon EC2 e Amazon ECS (incluso AWS Fargate), per rilevare potenziali minacce di runtime.
Protezione da malware per EC2	Rileva la potenziale presenza di malware eseguendo la scansione dei volumi Amazon EBS associati alle istanze Amazon EC2. È disponibile un'opzione per utilizzare questa funzionalità su richiesta.
Protezione da malware per S3	Rileva la potenziale presenza di malware negli oggetti appena caricati all'interno dei bucket Amazon S3. È disponibile un'opzione per utilizzare questa funzionalità su richiesta.
Protezione da malware per il AWS backup	Rileva la potenziale presenza di malware eseguendo la scansione delle risorse di backup, tra cui Snapshot EBS, AMI EC2 e punti di ripristino di Backup AWS . È disponibile un'opzione per utilizzare questa funzionalità su richiesta.
Protezione RDS	Analizza e profila la tua attività di accesso RDS per potenziali minacce di accesso ai database Amazon Aurora e Amazon RDS supportati.
Protezione Lambda	Monitora i registri delle attività della rete Lambda, a partire dai log di flusso VPC, per rilevare le minacce alle tue funzioni. AWS Lambda Esempi di queste potenziali minacce includono il cryptomining e la comunicazione con server dannosi.

 Abilita la protezione da malware per S3 in modo indipendente

GuardDuty offre la flessibilità necessaria per utilizzare Malware Protection for S3 in modo indipendente, senza abilitare il GuardDuty servizio Amazon. Per ulteriori

informazioni su come iniziare a utilizzare solo Malware Protection for S3, consulta [GuardDuty Protezione da malware per S3](#). Per utilizzare tutti gli altri piani di protezione, è necessario abilitare il GuardDuty servizio.

Gestisci un ambiente con più account

Puoi gestire un AWS ambiente con più account utilizzando il metodo di invito AWS Organizations (consigliato) o quello precedente. Per ulteriori informazioni, consulta [Account multipli in GuardDuty](#).

Genera risultati di sicurezza per le minacce rilevate

Quando GuardDuty rileva potenziali minacce alla sicurezza associate alle AWS risorse, inizia a generare risultati di sicurezza che forniscono informazioni sulla risorsa potenzialmente compromessa. Dopo averlo abilitato GuardDuty nel tuo account, genera [Risultati di esempio](#) per visualizzare il file associato. [Dettagli degli esiti](#) Per un elenco completo dei risultati di sicurezza, consulta [GuardDuty tipi di ricerca](#).

Con GuardDuty, puoi anche utilizzare uno script di tester che genera risultati GuardDuty di sicurezza specifici per capire come esaminare e rispondere ai GuardDuty risultati. Per ulteriori informazioni, consulta [GuardDuty Risultati dei test in account dedicati](#).

Valutazione e gestione dei risultati di sicurezza

GuardDuty consolida i risultati di sicurezza tra gli account e visualizza i risultati nella dashboard di riepilogo sulla GuardDuty console. Puoi anche recuperare i risultati tramite l' AWS Security Hub CSPM API o AWS l' AWS Command Line Interface SDK. Con una visione olistica del vostro attuale stato di sicurezza, potete identificare tendenze e potenziali problemi e adottare le misure correttive necessarie. Per ulteriori informazioni, consulta [Gestione dei GuardDuty risultati](#).

Integrazione con i servizi di sicurezza correlati AWS

Per aiutarvi ulteriormente ad analizzare e indagare sulle tendenze di sicurezza nel vostro AWS ambiente, prendete in considerazione l'utilizzo dei seguenti servizi AWS relativi alla sicurezza in combinazione con. GuardDuty

- AWS Security Hub CSPM— Questo servizio offre una visione completa dello stato di sicurezza delle AWS risorse e consente di controllare l' AWS ambiente rispetto agli standard e alle best practice del settore della sicurezza. Lo fa in parte consumando, aggregando, organizzando e dando priorità ai risultati di sicurezza provenienti da più AWS servizi (incluso Amazon Macie) e prodotti AWS Partner Network (APN) supportati. Security Hub CSPM consente di analizzare

le tendenze di sicurezza e identificare i problemi di sicurezza con la massima priorità in tutto l'AWS ambiente.

Per informazioni sull'utilizzo combinato GuardDuty di Security Hub CSPM, vedere [Integrazione con GuardDuty AWS Security Hub CSPM](#). Per ulteriori informazioni su Security Hub CSPM, consulta la Guida per l'[AWS Security Hub utente](#).

- Amazon Detective: questo servizio ti aiuta ad analizzare, indagare e identificare rapidamente la causa principale dei risultati di sicurezza o delle attività sospette. Detective raccoglie automaticamente i dati di registro dalle tue AWS risorse. Utilizza quindi il machine learning, l'analisi statistica e la teoria dei grafi per generare visualizzazioni che consentono di condurre indagini sulla sicurezza più rapide ed efficaci. Le aggregazioni, i riepiloghi e il contesto predefiniti di Detective ti aiutano ad analizzare e determinare la natura e l'entità dei potenziali problemi di sicurezza.

Per informazioni sull'uso combinato di Detective GuardDuty e Detective, vedere [Integrazione GuardDuty con Amazon Detective](#). Per ulteriori informazioni su Detective, consulta la [Amazon Detective User Guide](#).

- Amazon EventBridge: questo servizio ti aiuta a ricevere notifiche e rispondere ai risultati GuardDuty di sicurezza quasi in tempo reale. GuardDuty crea un evento in caso di modifica dei risultati. Puoi scegliere la frequenza da cui desideri ricevere le notifiche EventBridge. Per ulteriori informazioni, consulta [What is Amazon EventBridge](#) nella Amazon EventBridge User Guide.

Conformità PCI DSS

GuardDuty supporta l'elaborazione, l'archiviazione e la trasmissione dei dati delle carte di credito da parte di un commerciante o di un fornitore di servizi ed è stato convalidato come conforme al Payment Card Industry (PCI) Data Security Standard (DSS). Per ulteriori informazioni su PCI DSS, incluso come richiedere una copia del PCI AWS Compliance Package, vedere [PCI DSS Level 1](#).

Per ulteriori informazioni, consulta la sezione [Un nuovo test di terze parti confronta Amazon con i sistemi GuardDuty di rilevamento delle intrusioni di rete](#) nel AWS Security Blog.

Prezzi in GuardDuty

Questa sezione si concentra sul Piano gratuito di AWS modello GuardDuty utilizzato per i vari piani di protezione e su come visualizzare i costi di utilizzo stimati ed effettivi. Se stai cercando i dettagli sui prezzi associati a tutti i piani di protezione nelle regioni supportate, consulta [GuardDuty prezzi](#).

Piano gratuito di AWS

Piano gratuito di AWS ti aiuta a esplorare e provare Servizi AWS gratuitamente fino ai limiti specificati per ciascun servizio. Esistono tre categorie: 12 mesi di prova gratuita, sempre gratuita e prova gratuita a breve termine. Amazon GuardDuty appartiene alla categoria delle prove gratuite a breve termine e offre una prova gratuita di 30 giorni. Se continui a utilizzare al GuardDuty termine del periodo di prova gratuito, comincerai a incorrere in costi in base al modo in cui utilizzi questo servizio.

¹ Eccezione alla GuardDuty prova gratuita di 30 giorni

La scansione antimalware su richiesta (sotto Malware Protection for EC2) e Malware Protection for S3 non rientrano nella categoria delle versioni di prova gratuita a breve termine di GuardDuty 30 giorni. Malware Protection for S3 rientra nella categoria dei 12 mesi gratuiti, Piano gratuito di AWS mentre la scansione antimalware On-demand segue un modello di costo. pay-as-you-use Non è disponibile una prova gratuita di 30 giorni o un modello a costo gratuito di 12 mesi con scansione antimalware su richiesta.

Utilizzo GuardDuty della prova gratuita di 30 giorni

Quando si utilizza GuardDuty per la prima volta in un Regione AWS, Account AWS si viene automaticamente iscritti a una prova gratuita di 30 giorni in quella regione. Alcuni piani di protezione verranno inoltre abilitati automaticamente e sono inclusi nella prova gratuita di 30 giorni. Poiché si GuardDuty tratta di un servizio regionale, quando lo attivi per la prima volta in un'altra regione, il tuo account riceverà una prova gratuita di 30 giorni GuardDuty in quella regione. Quando lavori con più account in un' GuardDuty organizzazione, ogni account riceve la propria prova gratuita di 30 giorni.

Utilizza la tabella seguente per verificare quali piani di protezione sono abilitati di default e GuardDuty la loro disponibilità di prova gratuita.

Piano di protezione	Abilitato per impostazione predefinita con GuardDuty	Disponibilità di prova gratuita separata ²	
Protezione EKS	Sì	Sì	
Protezione S3	Sì	Sì	
Monitoraggio del runtime	No	Sì	
Protezione da malware per EC2 – GuardDuty-scansione antimalware avviata	Sì	Sì	
Protezione da malware per EC2 – Scansione antimalware su richiesta GuardDuty	No	No ¹	
GuardDuty Protezione da malware per S3	No	No ¹	
Protezione RDS	Sì	Sì	
Protezione Lambda	Sì	Sì	

² Quando si abilita GuardDuty per la prima volta, i piani di protezione (ad eccezione del Runtime Monitoring) vengono automaticamente abilitati e inclusi nella prova gratuita iniziale di 30 giorni. Quando un GuardDuty account esistente attiva un nuovo piano di protezione dopo la scadenza del periodo di prova GuardDuty gratuito iniziale, tale piano di protezione include una prova gratuita di 30 giorni. Per ulteriori informazioni sulle prove gratuite dei piani di protezione, consulta il documento associato a ciascun piano di protezione.

Visualizza i costi di utilizzo stimati durante la prova gratuita: durante la prova gratuita di 30 giorni GuardDuty e, potenzialmente, con un piano di protezione, GuardDuty fornisce il costo di utilizzo

stimato per il tuo account. Se sei un account GuardDuty amministratore delegato, puoi visualizzare il costo di utilizzo totale stimato e la ripartizione a livello di account per tutti gli account membro abilitati. GuardDuty Per ulteriori informazioni, consulta [Monitoraggio GuardDuty dell'utilizzo e stima dei costi](#).

Costo di utilizzo al termine del periodo di prova gratuito: se continui a utilizzare GuardDuty uno dei suoi piani di protezione dopo la fine del periodo di prova gratuito, inizierai a incorrere nei relativi costi di utilizzo. Per visualizzare la fattura, accedi a Cost Explorer nella <https://console.aws.amazon.com/costmanagement/console>. Per ulteriori informazioni sulla fatturazione AWS dell'account, consulta la [Guida per l'AWS Billing utente](#).

Utilizzo di Malware Protection for S3 con piano gratuito di 12 mesi

Malware Protection for S3 utilizza un piano gratuito associato al tuo piano Account AWS che può essere nuovo, con un piano gratuito continuativo o con un piano gratuito scaduto di 12 mesi. Per ulteriori informazioni, consulta [Prezzi e costi di utilizzo di Malware Protection for S3](#).

Accedendo GuardDuty

Amazon GuardDuty è disponibile nella maggior parte dei casi Regioni AWS. Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta [Regioni ed endpoint](#).

È possibile utilizzare GuardDuty in uno dei seguenti modi:

GuardDuty console

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

La console è un'interfaccia basata su browser che consente l'accesso a GuardDuty e il suo utilizzo. La GuardDuty console fornisce l'accesso all' GuardDuty account, ai dati e alle risorse.

AWS Command Line Interface

Con AWS Command Line Interface (AWS CLI), è possibile impartire comandi dalla riga di comando del sistema per eseguire GuardDuty attività e AWS attività. I AWS CLI comandi sono utili se desiderate creare script che eseguano operazioni.

Per informazioni sull'installazione e l'utilizzo AWS CLI, consulta la [Guida per AWS Command Line Interface l'utente](#). Per visualizzare i AWS CLI comandi disponibili per GuardDuty, vedere [AWS CLI Command Reference](#).

GuardDuty API HTTPS

Puoi GuardDuty accedervi in modo AWS programmatico utilizzando l'API GuardDuty HTTPS, che consente di inviare richieste HTTPS direttamente al servizio. Per ulteriori informazioni, consulta [Amazon GuardDuty API Reference](#).

AWS SDKs

AWS fornisce kit di sviluppo software (SDKs) costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Python, Ruby, .NET, iOS, Android e altro). SDKs Forniscono un modo conveniente per creare un accesso programmatico a. GuardDuty Per informazioni su AWS SDKs, incluso come scaricarli e installarli, consulta [Tools for Amazon Web Services](#).

Concetti e termini chiave in Amazon GuardDuty

Quando inizi a usare Amazon GuardDuty, puoi trarre vantaggio dalla conoscenza dei suoi concetti e dei termini chiave associati.

Account

Un account Amazon Web Services (AWS) standard che contiene AWS le tue risorse. Puoi accedere AWS con il tuo account e abilitare GuardDuty.

Puoi anche invitare altri account ad attivarsi GuardDuty e ad associarsi al tuo AWS account in GuardDuty. Se gli inviti vengono accettati, il tuo account viene designato come GuardDuty account amministratore e gli account aggiunti diventano i tuoi account membro. Puoi quindi visualizzare e gestire i GuardDuty risultati di tali account per loro conto.

Gli utenti dell'account amministratore possono configurare GuardDuty , visualizzare e gestire GuardDuty i risultati per il proprio account e per tutti gli account dei membri. Per informazioni sul numero di account membro che l'account amministratore può gestire, consulta [GuardDuty quote](#).

Gli utenti degli account membro possono configurare GuardDuty , visualizzare e gestire GuardDuty i risultati nel proprio account (tramite la console di GuardDuty gestione o l' GuardDuty API). Gli utenti degli account membri non possono consultare o gestire i risultati negli account degli altri membri.

Un non Account AWS può essere un account GuardDuty amministratore e un account membro allo stesso tempo. An Account AWS può accettare solo un invito all'iscrizione. L'accettazione di un invito è facoltativa.

Per ulteriori informazioni, consulta [Account multipli in Amazon GuardDuty](#).

Sequenze di attacco

Una sequenza di attacco è una correlazione di più eventi che, come osservato da GuardDuty, si sono verificati in una sequenza specifica che corrisponde allo schema di un'attività sospetta. GuardDuty utilizza la sua [Rilevamento esteso delle minacce](#) capacità di rilevare questi attacchi in più fasi che riguardano fonti di dati, AWS risorse e tempistiche fondamentali del tuo account.

L'elenco seguente illustra brevemente i termini chiave associati alle sequenze di attacco:

- Indicatori: fornisce informazioni sul motivo per cui una sequenza di eventi è in linea con una potenziale attività sospetta.

- **Segnali:** un segnale è un'attività API GuardDuty osservata o già rilevata nel GuardDuty tuo account. Correlando gli eventi osservati in una sequenza specifica nel tuo account, GuardDuty identifica una sequenza di attacco.

Nel tuo account ci sono eventi che non sono indicativi di una potenziale minaccia. GuardDuty li considera segnali deboli. Tuttavia, quando si osservano segnali e GuardDuty risultati deboli in una sequenza specifica che, se correlata, si allinea a un'attività potenzialmente sospetta, GuardDuty genera un rilevamento della sequenza di attacco.

- **Endpoint:** informazioni sugli endpoint di rete potenzialmente utilizzati da un autore della minaccia in una sequenza di attacco.

Rilevatore

Amazon GuardDuty è un servizio regionale. Quando GuardDuty abiliti uno specifico Regione AWS, il tuo Account AWS viene associato a un ID del rilevatore. Questo ID alfanumerico di 32 caratteri è unico per il tuo account in quella regione. Ad esempio, quando attivi GuardDuty lo stesso account in una regione diversa, il tuo account verrà associato a un ID rilevatore diverso. Il formato di un `detectorId` è `12abc34d567e8fa901bc2d34e56789f0`.

Tutti i GuardDuty risultati, gli account e le azioni relative alla gestione dei risultati e al GuardDuty servizio utilizzano l'ID del rilevatore per eseguire un'operazione API.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

Note

Negli ambienti con più account, viene eseguito il roll up degli esiti di ogni account membro fino al rilevatore dell'account amministratore.

Alcune GuardDuty funzionalità vengono configurate tramite il rilevatore, ad esempio la configurazione della frequenza di notifica CloudWatch degli eventi e l'attivazione o la disabilitazione di piani di protezione opzionali per l' GuardDuty elaborazione.

Utilizzo di Malware Protection for S3 all'interno GuardDuty

Quando abiliti Malware Protection for S3 in un account in cui GuardDuty è abilitata, le azioni di Malware Protection for S3 come l'attivazione, la modifica e la disabilitazione di una risorsa protetta non sono associate all'ID del rilevatore.

Se non abiliti GuardDuty e scegli l'opzione di rilevamento delle minacce Malware Protection for S3, non viene creato alcun ID di rilevamento per il tuo account.

Fonti di dati fondamentali

L'origine o la posizione di un set di dati. Per rilevare un'attività non autorizzata o imprevista nel proprio AWS ambiente. GuardDuty analizza ed elabora i dati dai registri degli AWS CloudTrail eventi, dagli eventi di AWS CloudTrail gestione, dagli eventi di AWS CloudTrail dati per S3, dai log di flusso VPC, dai registri DNS, vedi. [GuardDuty fonti di dati fondamentali](#)

Funzionalità

Un oggetto funzionale configurato per il piano di GuardDuty protezione consente di rilevare un'attività non autorizzata o imprevista nell' AWS ambiente. Ogni piano di GuardDuty protezione configura l'oggetto feature corrispondente per analizzare ed elaborare i dati. Alcuni degli oggetti delle funzionalità includono i registri di controllo EKS, il monitoraggio delle attività di accesso RDS, i registri delle attività di rete Lambda e i volumi EBS. Per ulteriori informazioni, consulta [Nomi delle funzionalità per i piani di protezione nell' GuardDuty API](#).

Risultato

Un potenziale problema di sicurezza rilevato da GuardDuty. Per ulteriori informazioni, consulta [Comprendere e generare i GuardDuty risultati di Amazon](#).

I risultati vengono visualizzati nella GuardDuty console e contengono una descrizione dettagliata del problema di sicurezza. Puoi anche recuperare i risultati generati chiamando le operazioni dell'[ListFindingsAPI](#) [GetFindings](#)and.

Puoi anche visualizzare i GuardDuty risultati tramite Amazon CloudWatch Events. GuardDuty invia i risultati ad Amazon CloudWatch tramite il protocollo HTTPS. Per ulteriori informazioni, consulta [Elaborazione dei GuardDuty risultati con Amazon EventBridge](#).

Ruolo IAM

Questo è il ruolo IAM con le autorizzazioni necessarie per scansionare l'oggetto S3. Quando l'etichettatura degli oggetti scansionati è abilitata, le PassRole autorizzazioni IAM aiutano ad GuardDuty aggiungere tag all'oggetto scansionato.

Risorsa del piano Malware Protection

Dopo aver abilitato Malware Protection for S3 per un bucket, GuardDuty crea una risorsa del piano Malware Protection. Questa risorsa è associata all'ID del piano Malware Protection, un identificatore univoco per il bucket protetto. Utilizza la risorsa del piano Malware Protection per eseguire operazioni API su una risorsa protetta.

Bucket protetto (risorsa protetta)

Un bucket Amazon S3 è considerato protetto quando si abilita Malware Protection for S3 per questo bucket e il suo stato di protezione cambia in Attivo.

GuardDuty supporta solo un bucket S3 come risorsa protetta.

Stato di protezione

Lo stato associato alla risorsa del piano Malware Protection. Dopo aver abilitato Malware Protection for S3 per il tuo bucket, questo stato indica se il bucket è configurato correttamente o meno.

Prefisso dell'oggetto S3

In un bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), puoi usare prefissi per organizzare lo storage. Un prefisso è un raggruppamento logico degli oggetti in un bucket S3. Per ulteriori informazioni, consulta [Organizing and listing objects](#) nella Amazon S3 User Guide.

Opzioni di scansione

Quando GuardDuty Malware Protection for EC2 è abilitato, consente di specificare quali EC2 istanze Amazon e volumi Amazon Elastic Block Store (EBS) scansionare o ignorare. Questa funzionalità consente di aggiungere i tag esistenti associati alle EC2 istanze e al volume EBS a un elenco di tag di inclusione o a un elenco di tag di esclusione. Le risorse associate ai tag che aggiungi a un elenco di tag di inclusione vengono analizzate alla ricerca di malware, mentre quelle associate a un elenco di tag di esclusione non vengono scansionate. Per ulteriori informazioni, consulta [Opzioni di scansione con tag definiti dall'utente](#).

Conservazione delle istantanee

Quando GuardDuty Malware Protection for EC2 è abilitato, offre la possibilità di conservare le istantanee dei volumi EBS nel tuo account. AWS GuardDuty genera i volumi EBS di replica in base alle istantanee dei volumi EBS. È possibile conservare le istantanee dei volumi EBS solo se Malware Protection for EC2 scan rileva malware nei volumi EBS di replica. Se non viene rilevato alcun malware nei volumi EBS di replica, elimina GuardDuty automaticamente le istantanee dei volumi EBS, indipendentemente dall'impostazione di conservazione delle istantanee. Per ulteriori informazioni, consulta [Conservazione delle istantanee](#).

Regola di soppressione

Le regole di soppressione automatica ti consentono di creare combinazioni di attributi molto specifiche per eliminare i risultati. Ad esempio, puoi definire una regola tramite il GuardDuty

filtro per archiviare automaticamente Recon: EC2/Portscan solo le istanze in un VPC specifico, eseguendo un'AMI specifica o con un tag specifico. EC2 Questa regola comporterebbe l'archiviazione automatica dei risultati di scansione delle porte dalle istanze che soddisfano i criteri. Tuttavia, consente comunque di inviare avvisi se GuardDuty rileva che le istanze svolgono altre attività dannose, come il mining di criptovalute.

Le regole di soppressione definite nell' GuardDuty account amministratore si applicano agli account dei membri. GuardDuty GuardDuty gli account membri non possono modificare le regole di soppressione.

Con le regole di soppressione, genera GuardDuty comunque tutti i risultati. Le regole di soppressione consentono di sopprimere i risultati mantenendo nel contempo uno storico non modificabile di tutte le attività.

In genere, le regole di soppressione vengono utilizzate per nascondere i risultati che sono stati determinati come falsi positivi per l'ambiente e ridurre il rumore derivante da risultati di basso valore, in modo da potersi concentrare sulle minacce più grandi. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

Elenco di indirizzi IP affidabili

Un elenco di indirizzi IP affidabili per comunicazioni altamente sicure con l' AWS ambiente in uso. GuardDuty non genera risultati basati su elenchi di IP affidabili. Per ulteriori informazioni, consulta [Personalizzazione del rilevamento delle minacce con elenchi di entità e elenchi di indirizzi IP](#).

Elenco di IP delle minacce

Un elenco degli indirizzi IP dannosi noti. Oltre a generare risultati a causa di un'attività potenzialmente sospetta, genera GuardDuty anche risultati basati su questi elenchi di minacce. Per ulteriori informazioni, consulta [Personalizzazione del rilevamento delle minacce con elenchi di entità e elenchi di indirizzi IP](#).

Guida introduttiva con GuardDuty

Questo tutorial fornisce un'introduzione pratica a. GuardDuty I requisiti minimi per l'abilitazione GuardDuty come account autonomo o come GuardDuty amministratore AWS Organizations sono descritti nella Fase 1. I passaggi da 2 a 5 riguardano l'utilizzo di funzionalità aggiuntive consigliate da GuardDuty per ottenere il massimo dai risultati.

Argomenti

- [Prima di iniziare](#)
- [Passaggio 1: abilitare Amazon GuardDuty](#)
- [Fase 2: generare esiti di esempio ed esplorare le operazioni di base](#)
- [Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3](#)
- [Passaggio 4: configura la GuardDuty ricerca di avvisi tramite SNS](#)
- [Fasi successive](#)

Prima di iniziare

GuardDuty è un servizio di rilevamento delle minacce che monitora [Origini dati fondamentali](#) eventi di AWS CloudTrail gestione, Amazon VPC Flow Logs Amazon Route 53 Resolver e log di query DNS. GuardDuty analizza anche le funzionalità associate ai suoi tipi di protezione solo se le abiliti separatamente. Le [funzionalità](#) includono log di controllo Kubernetes, attività di accesso RDS, eventi di dati AWS CloudTrail per Amazon S3, volumi Amazon EBS, Runtime Monitoring e registri delle attività di rete Lambda. L'utilizzo di queste fonti di dati e funzionalità (se abilitate), genera risultati di sicurezza per il tuo account. GuardDuty

Dopo l'attivazione GuardDuty, inizia a monitorare il tuo account alla ricerca di potenziali minacce in base alle attività nelle fonti di dati fondamentali. Per impostazione predefinita, [Rilevamento esteso delle minacce](#) è abilitato per tutti coloro Account AWS che sono abilitati GuardDuty. Questa funzionalità rileva sequenze di attacco in più fasi che riguardano più fonti di dati, AWS risorse e tempo fondamentali del tuo account. Per rilevare potenziali minacce a AWS risorse specifiche, puoi scegliere di abilitare piani di protezione incentrati sui casi d'uso che offrono. GuardDuty Per ulteriori informazioni, consulta [Caratteristiche di GuardDuty](#).

Non è necessario abilitare esplicitamente nessuna delle fonti di dati fondamentali. Quando abiliti S3 Protection, non è necessario abilitare esplicitamente la registrazione degli eventi dei dati di Amazon S3. Allo stesso modo, quando abiliti EKS Protection, non è necessario abilitare esplicitamente i log di

controllo di Amazon EKS. Amazon GuardDuty estrae flussi di dati indipendenti direttamente da questi servizi.

Per un nuovo GuardDuty account, alcuni dei tipi di protezione disponibili supportati in un Regione AWS sono abilitati e inclusi nel periodo di prova gratuito di 30 giorni per impostazione predefinita. È possibile disattivarne alcuni o tutti. Se ne hai già Account AWS GuardDuty attivato uno, puoi scegliere di abilitare uno o tutti i piani di protezione disponibili nella tua regione. Per una panoramica dei piani di protezione e dei piani di protezione che verranno attivati di default, consulta [Prezzi in GuardDuty](#).

Durante l'attivazione GuardDuty, considera i seguenti elementi:

- GuardDuty è un servizio regionale, il che significa che tutte le procedure di configurazione seguite in questa pagina devono essere ripetute in ogni regione con cui si desidera monitorare GuardDuty.

Ti consigliamo vivamente di abilitarlo GuardDuty in tutte le AWS regioni supportate. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche nelle Regioni che non utilizzi attivamente. Ciò consente inoltre di GuardDuty monitorare AWS CloudTrail gli eventi per AWS servizi globali come IAM. Se non GuardDuty è abilitato in tutte le regioni supportate, la sua capacità di rilevare attività che coinvolgono servizi globali è ridotta. Per un elenco completo delle regioni in cui GuardDuty è disponibile, consulta [Regioni ed endpoint](#).

- Qualsiasi utente con privilegi di amministratore in un AWS account può abilitare GuardDuty, tuttavia, seguendo la migliore pratica di sicurezza del privilegio minimo, si consiglia di creare un ruolo, un utente o un gruppo IAM da gestire GuardDuty in modo specifico. Per informazioni sulle autorizzazioni necessarie per l'attivazione, vedere. GuardDuty [Autorizzazioni necessarie per l'attivazione GuardDuty](#)
- Quando si abilita GuardDuty per la prima volta in qualsiasi regione Regione AWS, per impostazione predefinita, abilita anche tutti i tipi di protezione disponibili supportati in quella regione, inclusa Malware Protection for EC2. GuardDuty crea un ruolo collegato al servizio per il tuo account chiamato. `AWSServiceRoleForAmazonGuardDuty` Questo ruolo include le autorizzazioni e le politiche di fiducia che consentono GuardDuty di utilizzare e analizzare gli eventi direttamente dal [GuardDuty fonti di dati fondamentali](#) per generare risultati di sicurezza. Malware Protection for EC2 crea un altro ruolo collegato al servizio per l'account chiamato. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Questo ruolo include le autorizzazioni e le politiche di fiducia che consentono a Malware Protection for EC2 di eseguire scansioni senza agenti per rilevare il malware nel tuo account. GuardDuty Consente di GuardDuty creare un'istantanea del volume EBS nel tuo account e condividerla con l'account del servizio. GuardDuty Per ulteriori informazioni, consulta [Autorizzazioni di ruolo collegate al servizio per](#)

[GuardDuty](#). Per ulteriori informazioni sui ruoli collegati ai servizi, consulta [Utilizzo di ruoli collegati ai servizi](#).

- Quando lo attivi GuardDuty per la prima volta in qualsiasi regione, il tuo AWS account viene automaticamente registrato a una prova GuardDuty gratuita di 30 giorni per quella regione.

Il video seguente spiega come iniziare a utilizzare un account amministratore GuardDuty e attivarlo in più account membri.

[Guida introduttiva: abilitare Amazon GuardDuty per ambienti autonomi o con più account](#)

Passaggio 1: abilitare Amazon GuardDuty

Il primo passaggio per utilizzarlo GuardDuty è abilitarlo nel tuo account. Una volta abilitato, GuardDuty inizierà immediatamente a monitorare le minacce alla sicurezza nella regione corrente.

Se desideri gestire GuardDuty i risultati di altri account all'interno della tua organizzazione in qualità di GuardDuty amministratore, devi aggiungere e abilitare anche GuardDuty gli account dei membri.

 Note

Se desideri abilitare GuardDuty Malware Protection for S3 senza attivarlo GuardDuty, per la procedura, consulta [GuardDuty Protezione da malware per S3](#).

Standalone account environment

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>
2. Seleziona l'opzione Amazon GuardDuty - Tutte le funzionalità.
3. Scegli Avvia.
4. Nella GuardDuty pagina Benvenuto, visualizza i termini del servizio. Scegli Abilita GuardDuty.

Multi-account environment

 Important

Come prerequisiti per questo processo, devi appartenere alla stessa organizzazione di tutti gli account che desideri gestire e avere accesso all'account di AWS Organizations gestione per poter delegare un amministratore GuardDuty all'interno dell'organizzazione. Potrebbero essere necessarie autorizzazioni aggiuntive per delegare un amministratore. Per maggiori informazioni, consulta [Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty](#).

Per designare un account amministratore delegato GuardDuty

1. Apri la AWS Organizations console all'indirizzo <https://console.aws.amazon.com/organizations/>, utilizzando l'account di gestione.
2. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

È GuardDuty già abilitata nel tuo account?

- Se non GuardDuty è già abilitato, puoi selezionare Inizia e quindi designare un amministratore GuardDuty delegato nella pagina Benvenuto GuardDuty.
- Se GuardDuty è abilitato, puoi designare un amministratore GuardDuty delegato nella pagina Impostazioni.

3. Inserisci l'ID dell'account a dodici cifre dell' AWS account che desideri designare come amministratore delegato dell'organizzazione e scegli GuardDuty Delegato.

 Note

Se non GuardDuty è già abilitato, la designazione di un amministratore delegato lo abiliterà per quell'account nella regione corrente. GuardDuty

Per aggiungere account membri

Questa procedura prevede l'aggiunta di account membri a un account amministratore GuardDuty delegato tramite AWS Organizations. In alternativa è possibile aggiungere membri tramite invito. Per ulteriori informazioni su entrambi i metodi di associazione dei membri in GuardDuty, vedere.

[Account multipli in Amazon GuardDuty](#)

1. Accedere all'account amministratore delegato
2. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
3. Nel riquadro di navigazione, scegliere Settings (Impostazioni), quindi Accounts (Account).

Nella tabella account vengono visualizzati tutti gli account dell'organizzazione.

4. Scegli gli account che desideri aggiungere come membri selezionando la casella accanto all'ID account. Quindi, dal menu Operazione seleziona Aggiungi membro.

 Tip

Puoi automatizzare l'aggiunta di nuovi account come membri attivando la funzionalità di Abilitazione automatica, che però si applica solo agli account che entrano a far parte dell'organizzazione dopo l'abilitazione della funzionalità.

Fase 2: generare esiti di esempio ed esplorare le operazioni di base

Quando GuardDuty rileva un problema di sicurezza, genera un risultato. Un GuardDuty risultato è un set di dati contenente dettagli relativi a quell'unico problema di sicurezza. I dettagli dell'esito possono essere utilizzati per indagare sul problema.

GuardDuty supporta la generazione di risultati di esempio con valori segnaposto, che possono essere utilizzati per testare GuardDuty la funzionalità e acquisire familiarità con i risultati prima di dover rispondere a un problema di sicurezza reale scoperto da GuardDuty. Segui la guida riportata di seguito per generare risultati di esempio per ogni tipo di risultato disponibile. Per ulteriori modi per generare risultati di esempio GuardDuty, inclusa la generazione di un evento di sicurezza simulato all'interno del tuo account, consulta [Risultati di esempio](#).

Per creare ed esplorare gli esiti di esempio

1. Nel pannello di navigazione scegli Impostazioni.
2. Nella pagina Settings (Impostazioni), in Sample findings (Risultati di esempio), selezionare Generate sample findings (Genera risultati di esempio).
3. Nel riquadro di navigazione, scegli Riepilogo per visualizzare le informazioni dettagliate sui risultati generati nel tuo AWS ambiente. Per ulteriori informazioni sui componenti del pannello di Riepilogo, consulta [Dashboard di riepilogo in Amazon GuardDuty](#).
4. Nel riquadro di navigazione, seleziona Esiti. Gli esiti di esempio vengono visualizzati nella pagina Risultati attuali con il prefisso [ESEMPIO].
5. Seleziona un esito dall'elenco per visualizzarne i dettagli.
 - È possibile esaminare i diversi campi informativi disponibili nel riquadro dei dettagli degli esiti. Diversi tipi di esiti possono avere campi diversi. Per ulteriori informazioni sui campi disponibili in tutti i tipi di esiti, consulta [Dettagli degli esiti](#). Dal riquadro dei dettagli, puoi effettuare le operazioni seguenti:
 - Seleziona l'ID risultato nella parte superiore del riquadro per aprire i dettagli JSON completi dell'esito. Il file JSON completo può anche essere scaricato da questo pannello. Il file contiene alcune informazioni aggiuntive non incluse nella visualizzazione della console ed è in formato JSON, che può essere acquisito da altri strumenti e servizi.
 - Visualizza la sezione Risorsa interessata. Se si tratta di una scoperta reale, le informazioni qui riportate ti aiuteranno a identificare una risorsa nel tuo account che dovrebbe essere analizzata e includeranno collegamenti a risorse utili. Console di gestione AWS
 - Seleziona l'icona che raffigura una lente di ingrandimento con i simboli "+" o "-" per creare un filtro inclusivo o esclusivo per il dettaglio selezionato. Per ulteriori informazioni sui filtri per gli esiti, consulta [Filtrare i risultati in GuardDuty](#).
6. Archiviare tutti gli esiti di esempio

- a. Seleziona tutti gli esiti tramite la casella di controllo nella parte superiore dell'elenco.
- b. Deseleziona gli esiti che desideri conservare.
- c. Seleziona il menu Operazioni, quindi scegli Archivia per nascondere gli esiti di esempio.

 Note

Per visualizzare gli esiti archiviati, seleziona Correnti, quindi Archiviati per cambiare la visualizzazione degli esiti.

Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3

GuardDuty consiglia di configurare le impostazioni per esportare i risultati perché consente di esportare i risultati in un bucket S3 per l'archiviazione a tempo indeterminato oltre il periodo di conservazione di 90 giorni. GuardDuty Ciò consente di tenere traccia dei risultati o tenere traccia dei problemi all'interno del proprio ambiente nel tempo. AWS GuardDuty crittografa i dati dei risultati nel bucket S3 utilizzando AWS Key Management Service (AWS KMS). Per configurare le impostazioni, è necessario fornire GuardDuty all'autorizzazione una chiave KMS. Per passaggi più dettagliati, consulta [Esportazione dei risultati generati su Amazon S3](#).

Per esportare GuardDuty i risultati nel bucket Amazon S3

1. Allega la policy alla chiave KMS
 - a. Accedi a Console di gestione AWS e apri la console AWS Key Management Service (AWS KMS) in <https://console.aws.amazon.com/kms>.
 - b. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
 - c. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
 - d. Seleziona una chiave KMS esistente o esegui i passaggi per [creare una chiave KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori AWS Key Management Service

La regione della chiave KMS e del bucket Amazon S3 devono coincidere.

Copia la chiave ARN su un blocco note per utilizzarla nei passaggi successivi.

- e. Nella sezione Politica delle chiavi della tua chiave KMS, scegli Modifica. Se è visualizzata la visualizzazione Passa alla politica, selezionala per visualizzare la politica chiave, quindi scegli Modifica.
- f. Copia il seguente blocco di policy nella tua policy chiave 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"
    }
  }
}
```

Modifica la politica sostituendo i seguenti valori formattati *red* nell'esempio di policy:

1. Sostituisci *KMS key ARN* con l'Amazon Resource Name (ARN) della chiave KMS. Per individuare l'ARN della chiave, consulta [Finding the key ID and ARN](#) nella Developer Guide.AWS Key Management Service
2. *123456789012* Sostituiscilo con l' Account AWS ID proprietario dell' GuardDuty account che esporta i risultati.
3. Sostituisci *Region2* con il Regione AWS luogo in cui vengono generati i GuardDuty risultati.
4. Sostituisci *SourceDetectorID* con l' GuardDuty account detectorID della regione specifica in cui sono stati generati i risultati.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

2. Allega la policy al bucket Amazon S3

Se non disponi già di un bucket Amazon S3 in cui esportare questi risultati, consulta [Creating a bucket](#) nella Amazon S3 User Guide.

- a. Esegui i passaggi indicati in [Per creare o modificare una policy sui bucket](#) nella Guida per l'utente di Amazon S3, finché non viene visualizzata la pagina Modifica policy del bucket.
- b. La policy di esempio mostra come concedere GuardDuty l'autorizzazione all'esportazione dei risultati nel bucket Amazon S3. Se modifichi il percorso dopo aver configurato i risultati di esportazione, devi modificare la politica per concedere l'autorizzazione alla nuova posizione.

Copia la seguente politica di esempio e incollala nell'editor delle politiche Bucket.

Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la sintassi JSON della tua politica delle chiavi KMS sia valida.

Esempio di politica del bucket 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. Modifica la politica sostituendo i seguenti valori formattati *red* nell'esempio di policy:

1. Sostituisci *Amazon S3 bucket ARN* con l'Amazon Resource Name (ARN) del bucket Amazon S3. Puoi trovare il Bucket ARN nella pagina Modifica policy del bucket nella console. <https://console.aws.amazon.com/s3/>
2. *123456789012* Sostituiscilo con l' Account AWS ID proprietario dell' GuardDuty account che esporta i risultati.
3. Sostituisci *Region2* con il Regione AWS luogo in cui vengono generati i GuardDuty risultati.
4. Sostituisci *SourceDetectorID* con l' GuardDuty account detectorID della regione specifica in cui sono stati generati i risultati.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

5. Sostituisci *[optional prefix]* parte del valore del *S3 bucket ARN/[optional prefix]* segnaposto con una posizione di cartella opzionale in cui desideri esportare i

risultati. Per ulteriori informazioni sull'uso dei prefissi, consulta [Organizing objects using prefixes](#) nella Amazon S3 User Guide.

Se fornisci una posizione opzionale per la cartella che non esiste già, la GuardDuty creerà solo se l'account associato al bucket S3 è lo stesso dell'account che esporta i risultati. Quando esporti i risultati in un bucket S3 che appartiene a un altro account, la posizione della cartella deve già esistere.

6. Sostituisci **KMS key ARN** con l'Amazon Resource Name (ARN) della chiave KMS associata alla crittografia dei risultati esportati nel bucket S3. Per individuare l'ARN della chiave, consulta [Finding the key ID and ARN](#) nella Developer Guide.AWS Key Management Service

3. Passaggi nella console GuardDuty

- a. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
- b. Nel pannello di navigazione scegli Impostazioni.
- c. Nella pagina Impostazioni, in Opzioni di esportazione di Findings, per il bucket S3, scegli Configura ora (o Modifica, se necessario).
- d. Per l'ARN del bucket S3, inserisci **bucket ARN** quello a cui desideri inviare i risultati. Per visualizzare l'ARN del bucket, [consulta Visualizzazione delle proprietà di un bucket S3 nella Amazon S3](#) User Guide.
- e. Per l'ARN della chiave KMS, inserisci **key ARN** Per individuare l'ARN della chiave, consulta [Find the key ID and key ARN](#) nella Developer Guide.AWS Key Management Service
- f. Scegli Save (Salva).

Passaggio 4: configura la GuardDuty ricerca di avvisi tramite SNS

GuardDuty si integra con Amazon EventBridge, che può essere utilizzato per inviare i dati dei risultati ad altre applicazioni e servizi per l'elaborazione. Con EventBridge puoi utilizzare GuardDuty i risultati per avviare risposte automatiche ai tuoi risultati collegando gli eventi di ricerca a obiettivi come AWS Lambda funzioni, automazione di Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) e altro ancora.

In questo esempio creerai un argomento SNS come obiettivo di una EventBridge regola, quindi lo utilizzerai EventBridge per creare una regola da cui acquisire i dati dei risultati. GuardDuty La regola risultante inoltra i dettagli degli esiti a un indirizzo e-mail. Per scoprire come inviare gli esiti a Slack o

Amazon Chime e come modificare i tipi di esiti per cui vengono inviati gli avvisi, consulta [Configurare un argomento e un endpoint di Amazon SNS](#).

Per creare un argomento SNS per gli avvisi sugli esiti

1. [Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
2. Nel pannello di navigazione, scegli Argomenti.
3. Seleziona Create Topic (Crea argomento).
4. Per Tipo, seleziona Standard.
5. Per Nome, immetti **GuardDuty**.
6. Seleziona Create Topic (Crea argomento). Verranno aperti i dettagli dell'argomento per il nuovo argomento.
7. Nella sezione Subscriptions (Sottoscrizioni) scegliere Create subscription (Crea sottoscrizione).
8. Per Protocollo, scegli E-mail.
9. Per Endpoint, inserisci l'indirizzo e-mail a cui desideri che vengano inviate le notifiche.
10. Scegli Create Subscription (Crea sottoscrizione).

Dopo aver creato la sottoscrizione è necessario confermarla tramite e-mail.

11. Per verificare la presenza di un messaggio di sottoscrizione, vai alla tua casella di posta elettronica e nel messaggio di sottoscrizione scegli Conferma sottoscrizione.

 Note

Per verificare lo status dell'e-mail di conferma, vai alla console SNS e scegli Sottoscrizioni.

Per creare una EventBridge regola per acquisire i GuardDuty risultati e formattarli

1. Apri la EventBridge console all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.

Una regola non può avere lo stesso nome di un'altra regola nella stessa Regione e sullo stesso router di eventi.

5. Per Event bus (Bus di eventi), scegli default.
6. Per Tipo di regola, scegli Regola con un modello di eventi.
7. Scegli Next (Successivo).
8. Per Event source (Origine eventi), seleziona AWS events (Eventi).
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per Servizio AWS , scegli GuardDuty.
12. Per Tipo di evento, scegli GuardDutyRicerca.
13. Scegli Next (Successivo).
14. Per Tipi di destinazione, scegli servizio AWS .
15. Per Seleziona una destinazione, scegli Argomento SNS e per Argomento, scegli il nome dell'argomento SNS che hai creato in precedenza.
16. Nella sezione Impostazioni aggiuntive, per Configura input di destinazione, scegli Trasformatore di input.

L'aggiunta di un trasformatore di input formatta i dati di ricerca JSON inviati GuardDuty in un messaggio leggibile dall'uomo.

17. Seleziona Configura il trasformatore di input.
18. Nella sezione Trasformatore di input di destinazione, in Percorso di input, incolla il codice seguente:

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

19. Per formattare l'e-mail, in Template, incolla il codice seguente e assicurati di sostituire il testo in rosso con i valori appropriati alla tua regione:

```
"You have a severity severity GuardDuty finding type Finding_Type in
the Region_Name Region."
```

"Finding Description:"

"*Finding_Description*."

"For more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?region=region#/findings?search=id%3DFinding_ID"

20. Scegli Conferma.
21. Scegli Next (Successivo).
22. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i [EventBridge tag Amazon](#) nella Amazon EventBridge User Guide.
23. Scegli Next (Successivo).
24. Rivedi i dettagli della regola e scegli Crea regola.
25. (Facoltativo) Testa la tua nuova regola generando esiti di esempio con il processo descritto nella fase 2. Riceverai un'e-mail per ogni esito di esempio generato.

Fasi successive

Continuando a utilizzare GuardDuty, imparerai a comprendere i tipi di risultati pertinenti al tuo ambiente. Ogni volta che ricevi un nuovo esito, puoi trovare diverse informazioni, come i consigli su come correggerlo, selezionando Ulteriori informazioni dalla descrizione nel riquadro dei dettagli degli esiti o cercando il nome dell'esito su [GuardDuty tipi di ricerca](#).

Le seguenti funzionalità ti aiuteranno a ottimizzare GuardDuty in modo che possa fornire i risultati più pertinenti per il tuo AWS ambiente:

- Per ordinare facilmente i risultati in base a criteri specifici, come l'ID dell'istanza, l'ID dell'account, il nome del bucket S3 e altro, puoi creare e salvare filtri all'interno. GuardDuty Per ulteriori informazioni, consulta [Filtrare i risultati in GuardDuty](#).
- Se ricevi esiti relativi al comportamento previsto nel tuo ambiente, puoi archivarli automaticamente in base ai criteri definiti con le [regole di eliminazione](#).
- Per evitare che i risultati vengano generati da un sottoinsieme di siti affidabili IPs o per far sì che il GuardDuty monitoraggio IPs non rientri nel normale ambito di monitoraggio, puoi impostare elenchi di [indirizzi IP e minacce affidabili](#).

GuardDuty fonti di dati fondamentali

GuardDuty utilizza le fonti di dati di base per rilevare le comunicazioni con domini e indirizzi IP dannosi noti e identificare comportamenti potenzialmente anomali e attività non autorizzate. Durante il transito da queste fonti a GuardDuty, tutti i dati di registro vengono crittografati. GuardDuty estrae vari campi da queste fonti di log per la profilazione e il rilevamento delle anomalie, quindi elimina questi registri.

Quando si abilita GuardDuty per la prima volta in una regione, è disponibile una prova gratuita di 30 giorni che include il rilevamento delle minacce per tutte le fonti di dati di base. Durante questa prova gratuita, puoi monitorare un utilizzo mensile stimato suddiviso per ciascuna fonte di dati fondamentale. In qualità di account GuardDuty amministratore delegato, puoi visualizzare il costo di utilizzo mensile stimato suddiviso per ogni account membro che appartiene alla tua organizzazione e che è stato abilitato. GuardDuty Al termine del periodo di prova di 30 giorni, puoi utilizzarlo AWS Billing per ottenere informazioni sul costo di utilizzo.

Non sono previsti costi aggiuntivi per l' GuardDuty accesso agli eventi e ai log da queste fonti di dati fondamentali.

Dopo averlo abilitato GuardDuty Account AWS, inizia automaticamente a monitorare le fonti di registro spiegate nelle sezioni seguenti. Non è necessario abilitare nient'altro per iniziare GuardDuty ad analizzare ed elaborare queste fonti di dati per generare i risultati di sicurezza associati.

Argomenti

- [AWS CloudTrail eventi di gestione](#)
- [Log di flusso VPC](#)
- [Registri delle query DNS di Route53 Resolver](#)

AWS CloudTrail eventi di gestione

AWS CloudTrail fornisce una cronologia delle chiamate AWS API per il tuo account, incluse le chiamate API effettuate utilizzando gli Console di gestione AWS strumenti a riga di comando e determinati AWS servizi. AWS SDKs CloudTrail consente inoltre di identificare gli utenti e gli account richiamati AWS APIs per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state richiamate le chiamate e l'ora in cui sono state richiamate le chiamate. Per ulteriori informazioni, consulta [Che cos'è AWS CloudTrail?](#) nella Guida per l'utente di AWS CloudTrail .

GuardDuty monitora gli eventi CloudTrail di gestione, noti anche come eventi del piano di controllo. Questi eventi forniscono informazioni dettagliate sulle operazioni di gestione eseguite sulle risorse dell'azienda. Account AWS

Di seguito sono riportati alcuni esempi di eventi di CloudTrail gestione GuardDuty monitorati:

- Configurazione della sicurezza (operazioni dell'AttachRolePolicyAPI IAM)
- Configurazione delle regole per il routing dei dati (Amazon EC2 CreateSubnet API operations)
- Configurazione della registrazione (operazioni API)AWS CloudTrail CreateTrail

Quando viene abilitata GuardDuty, inizia a consumare gli eventi di CloudTrail gestione direttamente CloudTrail attraverso un flusso di eventi indipendente e duplicato e analizza i CloudTrail registri degli eventi.

GuardDuty non gestisce CloudTrail gli eventi né influisce sulle configurazioni esistenti. CloudTrail Allo stesso modo, le CloudTrail configurazioni non influiscono sul modo in cui GuardDuty utilizza ed elabora i registri degli eventi. Per gestire l'accesso e la conservazione dei tuoi CloudTrail eventi, utilizza la console di CloudTrail servizio o l'API. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#) nella Guida AWS CloudTrail per l'utente.

Come GuardDuty gestisce gli eventi AWS CloudTrail globali

Per la maggior parte AWS dei servizi, CloudTrail gli eventi vengono registrati nel Regione AWS luogo in cui vengono creati. Per i servizi globali come AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), CloudFront Amazon e Amazon Route 53 (Route 53), gli eventi vengono generati solo nella regione in cui si verificano, ma hanno un'importanza globale.

Quando GuardDuty utilizza [eventi di servizio CloudTrail globali](#) (GSE) con valori di sicurezza come configurazioni di rete o autorizzazioni utente, replica tali eventi e li elabora in ogni regione in cui sono stati abilitati. GuardDuty Questo comportamento aiuta a GuardDuty mantenere i profili utente e di ruolo in ogni regione, il che è fondamentale per rilevare eventi anomali.

Note

Per i risultati generati da questi eventi di servizio globali, il valore della regione nel risultato può differire dalla regione in cui GuardDuty viene creato il rilevamento. Ad esempio, un

risultato potrebbe essere visualizzato us-east-1 come Regione anche se GuardDuty crea il rilevamento in una regione diversa.

Ti consigliamo di abilitare GuardDuty tutte le Regioni AWS opzioni disponibili nel tuo Account AWS. Anche se non disponi di risorse distribuite in determinate regioni, l'attivazione GuardDuty aiuta a proteggere il tuo account da potenziali minacce. Gli autori delle minacce possono potenzialmente lanciare attacchi tramite servizi globali (come IAM o Amazon CloudFront). AWS STS Possono tentare di creare risorse non autorizzate per sfruttare le regioni in cui la presenza dell'utente è limitata. GuardDuty elabora eventi di servizio globali in tutte le regioni in cui è stato abilitato il servizio, incluse le regioni predefinite e quelle con consenso esplicito. Ciò aiuta a GuardDuty rilevare attività potenzialmente sospette in tutte le regioni Account AWS, comprese le regioni in cui non si utilizzano attivamente le risorse.

Log di flusso VPC

La funzionalità VPC Flow Logs di Amazon VPC acquisisce informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete collegate alle istanze Amazon Elastic Compute Cloud (Amazon) all'interno del tuo ambiente. EC2 AWS

Quando lo abiliti GuardDuty, inizia immediatamente ad analizzare i log di flusso VPC dalle istanze EC2 Amazon all'interno del tuo account. Utilizza gli eventi del log di flusso VPC direttamente dalla funzionalità VPC Flow Logs attraverso un flusso indipendente e duplicato di log di flusso. Questo processo non altera alcuna configurazione di log di flusso esistente.

[Protezione Lambda](#)

Lambda Protection è un miglioramento opzionale di Amazon. GuardDuty Attualmente, il monitoraggio delle attività di rete Lambda include i log di flusso di Amazon VPC di tutte le funzioni Lambda del tuo account, anche quelli che non utilizzano reti VPC. Per proteggere la tua funzione Lambda da potenziali minacce alla sicurezza, dovrai configurare Lambda Protection nel tuo account. GuardDuty Per ulteriori informazioni, consulta [Protezione Lambda](#).

[GuardDuty monitoraggio del runtime](#)

Quando gestisci il security agent (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring per EC2 istanze e GuardDuty viene attualmente distribuito su un' EC2 istanza Amazon e riceve i dati [Tipi di eventi di runtime raccolti](#) da questa istanza, non GuardDuty

ti verrà addebitato alcun costo Account AWS per l'analisi dei log di flusso VPC da questa istanza Amazon. EC2 Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

GuardDuty non gestisce i log di flusso né li rende accessibili nel tuo account. Per gestire l'accesso dei log di flusso e la loro conservazione, devi configurare la funzionalità Log di flusso VPC.

Registri delle query DNS di Route53 Resolver

Se utilizzi resolver AWS DNS per le tue EC2 istanze Amazon (l'impostazione predefinita), GuardDuty puoi accedere ed elaborare la tua richiesta e rispondere ai log delle query DNS di Route53 Resolver tramite i resolver DNS interni. AWS Se utilizzi un altro resolver DNS, come OpenDNS o GoogleDNS, o se configuri i tuoi resolver DNS, non puoi accedere ed elaborare i dati da questa fonte di dati. GuardDuty

Quando lo abiliti GuardDuty, inizia immediatamente ad analizzare i log delle query DNS di Route53 Resolver da un flusso di dati indipendente. Questo flusso di dati è separato dai dati forniti tramite la funzionalità di [Registrazione delle query del Route 53 Resolver](#). La configurazione di questa funzionalità non influisce sull'analisi. GuardDuty

Note

GuardDuty non supporta il monitoraggio dei log DNS per EC2 le istanze Amazon avviate su AWS Outposts perché la funzionalità di registrazione delle Amazon Route 53 Resolver query non è disponibile in quell'ambiente.

GuardDuty Rilevamento esteso delle minacce

GuardDuty Extended Threat Detection rileva automaticamente gli attacchi in più fasi che riguardano fonti di dati, più tipi di AWS risorse e tempi, all'interno di un unico Account AWS. Grazie a questa funzionalità, GuardDuty si concentra sulla sequenza di più eventi che osserva monitorando diversi tipi di fonti di dati. Extended Threat Detection mette in correlazione questi eventi per identificare gli scenari che si presentano come una potenziale minaccia per l'AWS ambiente e quindi genera una ricerca della sequenza di attacco.

Argomenti

- [Esempi di scenari di minaccia relativi alla sequenza di attacco](#)
- [Come funziona](#)
- [Attivazione di piani di protezione per massimizzare il rilevamento delle minacce](#)
- [Rilevamento esteso delle minacce nella console GuardDuty](#)
- [Comprensione e gestione dei risultati della sequenza di attacco](#)
- [Risorse aggiuntive](#)

Esempi di scenari di minaccia relativi alla sequenza di attacco

Extended Threat Detection copre scenari di minaccia che comportano compromissioni legate all'uso improprio AWS delle credenziali, tentativi di compromissione dei dati nei bucket Amazon S3 e compromissione di container e risorse Kubernetes nei cluster Amazon EKS. Una singola scoperta può comprendere un'intera sequenza di attacco. Ad esempio, l'elenco seguente descrive gli scenari che GuardDuty potrebbero rilevare:

Esempio 1: compromissione AWS delle credenziali e dei dati del bucket Amazon S3

- Un autore di minacce che ottiene l'accesso non autorizzato a un carico di lavoro di elaborazione.
- L'attore esegue quindi una serie di azioni come aumentare i privilegi e stabilire la persistenza.
- Infine, l'attore che esfiltra dati da una risorsa Amazon S3.

Esempio 2: compromissione del cluster Amazon EKS

- Un autore di minacce tenta di sfruttare un'applicazione container all'interno di un cluster Amazon EKS.

- L'attore utilizza quel contenitore compromesso per ottenere token di account di servizio privilegiati.
- L'attore sfrutta quindi questi privilegi elevati per accedere a segreti o risorse Kubernetes sensibili tramite le identità dei pod. AWS

A causa della natura degli scenari di minaccia associati, considera tutti elementi critici. GuardDuty [tipi di ricerca delle sequenze di attacco](#)

Il video seguente fornisce una dimostrazione di come utilizzare Extended Threat Detection.

[Dimostrazione di Amazon GuardDuty Extended Threat Detection](#)

Come funziona

Quando abiliti Amazon GuardDuty nel tuo account in una specifica Regione AWS, anche Extended Threat Detection è abilitato per impostazione predefinita. Non sono previsti costi aggiuntivi associati all'utilizzo di Extended Threat Detection. Per impostazione predefinita, mette in correlazione tutti [Origini dati fondamentali](#) gli eventi. Tuttavia, abilitando più piani di GuardDuty protezione, come S3 Protection, EKS Protection e Runtime Monitoring, si apriranno ulteriori tipi di rilevamenti delle sequenze di attacco ampliando la gamma di fonti di eventi. Ciò contribuirà potenzialmente a un'analisi

delle minacce più completa e a un migliore rilevamento delle sequenze di attacco. Per ulteriori informazioni, consulta [Attivazione di piani di protezione per massimizzare il rilevamento delle minacce](#).

GuardDuty mette in correlazione più eventi, tra cui le attività e GuardDuty i risultati delle API. Questi eventi sono chiamati segnali. A volte, possono verificarsi eventi nell'ambiente che, di per sé, non si presentano come una potenziale minaccia evidente. GuardDuty li definisce segnali deboli. Con Extended Threat Detection, GuardDuty identifica quando una sequenza di più azioni si allinea a un'attività potenzialmente sospetta e genera una sequenza di attacco rilevata nel tuo account. Queste azioni multiple possono includere segnali deboli e GuardDuty risultati già identificati nel tuo account.

Note

Quando mette in correlazione gli eventi per le sequenze di attacco, Extended Threat Detection non prende in considerazione i risultati archiviati, compresi quelli che vengono archiviati automaticamente a causa di. [Regole di eliminazione](#) Questo comportamento garantisce che solo i segnali attivi e pertinenti contribuiscano al rilevamento della sequenza di attacco. Per assicurarti che ciò non influisca su di te, consulta le regole di soppressione esistenti nel tuo account. Per ulteriori informazioni, consulta [Utilizzo delle regole di soppressione con Extended Threat Detection](#).

GuardDuty è inoltre progettato per identificare potenziali comportamenti di attacco in corso o recenti (entro una finestra temporale di 24 ore) nel tuo account. Ad esempio, un attacco potrebbe iniziare quando un attore accede involontariamente a un carico di lavoro di elaborazione. L'attore eseguirebbe quindi una serie di passaggi, tra cui l'enumerazione, l'aumento dei privilegi e l'esfiltrazione delle credenziali. AWS Queste credenziali potrebbero essere potenzialmente utilizzate per ulteriori compromissioni o accessi malintenzionati ai dati.

Attivazione di piani di protezione per massimizzare il rilevamento delle minacce

Extended Threat Detection è abilitato automaticamente per tutti GuardDuty gli account, valutando per impostazione predefinita i segnali provenienti da tutti i piani di protezione abilitati nell'account. GuardDuty [Le fonti di dati di base](#) forniscono segnali importanti per il rilevamento di diverse sequenze di attacchi. Ad esempio, con il rilevamento delle minacce di base, è GuardDuty possibile identificare una potenziale sequenza di attacco a partire dall'attività di individuazione dei privilegi IAM su Amazon

APIs S3 e rilevare le successive alterazioni del piano di controllo S3, come le modifiche che rendono la policy delle risorse del bucket più permissiva. Tuttavia, altre sequenze di attacco richiedono segnali avanzati che sono disponibili solo tramite piani di protezione avanzati come Runtime Monitoring, S3 Protection e EKS Audit Log Monitoring.

Argomenti

- [Rilevamento delle sequenze di attacco nei cluster Amazon EKS](#)
- [Rilevamento delle sequenze di attacco nei bucket Amazon S3](#)
- [Rilevamento delle sequenze di attacco nei cluster Amazon ECS](#)
- [Rilevamento delle sequenze di attacco nei gruppi di istanze Amazon EC2](#)

Rilevamento delle sequenze di attacco nei cluster Amazon EKS

GuardDuty ha correlato più segnali di sicurezza tra i log di controllo EKS, il comportamento di runtime dei processi e l'attività delle AWS API per rilevare modelli di attacco sofisticati. Per trarre vantaggio da Extended Threat Detection for EKS, è necessario abilitare almeno una di queste funzionalità: EKS Protection o Runtime Monitoring (con componente aggiuntivo EKS). EKS Protection monitora le attività del piano di controllo tramite registri di controllo, mentre Runtime Monitoring osserva i comportamenti all'interno dei container.

Per la massima copertura e un rilevamento completo delle minacce, GuardDuty consiglia di abilitare entrambi i piani di protezione. Insieme, creano una visione completa dei cluster EKS, che consente di GuardDuty rilevare modelli di attacco complessi. Ad esempio, può identificare un'implementazione anomala di un contenitore privilegiato (rilevata con EKS Protection), seguita da tentativi di persistenza, crypto-mining e creazione di shell inverse all'interno di quel contenitore (rilevata con Runtime Monitoring). GuardDuty rappresenta questi eventi correlati come un'unica rilevazione di gravità critica, denominata. [AttackSequence:EKS/CompromisedCluster](#) Quando si abilitano entrambi i piani di protezione, la ricerca della sequenza di attacco copre i seguenti scenari di minaccia:

- Compromissione dei container che eseguono applicazioni web vulnerabili
- Accesso non autorizzato tramite credenziali configurate in modo errato
- Tentativi di aumentare i privilegi
- Richieste API sospette
- Tentativi di accesso intenzionale ai dati

L'elenco seguente fornisce dettagli su quando questi piani di protezione dedicati sono abilitati singolarmente:

Protezione EKS

L'abilitazione di EKS Protection offre GuardDuty la possibilità di rilevare sequenze di attacco che coinvolgono le attività del piano di controllo del cluster Amazon EKS. Ciò consente di GuardDuty correlare i log di controllo EKS e l'attività delle AWS API. Ad esempio, GuardDuty può rilevare una sequenza di attacco in cui un attore tenta di accedere non autorizzato ai segreti del cluster, modifica le autorizzazioni di controllo degli accessi basate sui ruoli (RBAC) di Kubernetes e crea pod privilegiati. Per ulteriori informazioni [Protezione EKS](#) sull'attivazione di questo piano di protezione, consulta.

Monitoraggio del runtime per Amazon EKS

L'abilitazione del Runtime Monitoring per i cluster Amazon EKS offre GuardDuty la possibilità di migliorare il rilevamento della sequenza di attacco EKS con visibilità a livello di contenitore. Questo aiuta a GuardDuty rilevare potenziali processi dannosi, comportamenti di runtime sospetti e la potenziale esecuzione di malware. Ad esempio, GuardDuty è in grado di rilevare una sequenza di attacco in cui un contenitore inizia a mostrare comportamenti sospetti, come processi di cryptomining o stabilire connessioni a endpoint dannosi noti. Per ulteriori informazioni sull'attivazione di questo piano di protezione, consulta. [Monitoraggio del runtime](#)

Se non abiliti EKS Protection o Runtime Monitoring, non GuardDuty sarà possibile generare singoli [Tipi di risultati di protezione EKS](#) o [Tipi di risultati del monitoraggio del runtime](#). Pertanto, non GuardDuty sarà in grado di rilevare sequenze di attacchi in più fasi che coinvolgono risultati associati.

Rilevamento delle sequenze di attacco nei bucket Amazon S3

L'attivazione di S3 Protection offre GuardDuty la possibilità di rilevare sequenze di attacco che comportano tentativi di compromissione dei dati nei bucket Amazon S3. Senza S3 Protection, GuardDuty può rilevare quando la politica sulle risorse del bucket S3 diventa eccessivamente permissiva. Quando abiliti S3 Protection, GuardDuty acquisisce la capacità di rilevare potenziali attività di esfiltrazione dei dati che potrebbero verificarsi dopo che il bucket S3 diventa eccessivamente permissivo.

Se S3 Protection non è abilitato, non sarà in grado di generare dati individuali. GuardDuty [Tipi di risultati di protezione S3](#) Pertanto, non GuardDuty sarà in grado di rilevare sequenze di attacchi in

più fasi che coinvolgono risultati associati. Per ulteriori informazioni sull'attivazione di questo piano di protezione, vedere. [Protezione S3](#)

Rilevamento delle sequenze di attacco nei cluster Amazon ECS

GuardDuty è in grado di identificare sequenze di attacco come processi dannosi, connessioni a endpoint dannosi o comportamenti di crypto-mining all'interno dei contenitori ECS. Correlando diversi segnali tra l'attività di rete, il comportamento di esecuzione dei processi e l'attività delle AWS API, è in GuardDuty grado di identificare modelli di attacco complessi che potrebbero non essere rilevati dai singoli rilevamenti e mappare il vettore di attacco completo.

GuardDuty rappresenta questi eventi correlati come un'unica rilevazione di gravità critica, denominata. `AttackSequence:ECS/CompromisedCluster` L'individuazione della sequenza di attacco copre i seguenti scenari di minaccia:

- Compromissione dei container che eseguono servizi vulnerabili
- Esecuzione non autorizzata di strumenti, malware o processi di cryptomining sospetti
- Tentativi di aumentare i privilegi
- Comunicazione con endpoint sospetti

Important

Extended Threat Detection for ECS richiede Runtime Monitoring for Fargate o EC2, a seconda del tipo di infrastruttura ECS. Runtime Monitoring osserva i comportamenti all'interno dei container ECS in esecuzione su istanze Fargate ed EC2. ECS sulle istanze EC2 gestite non è supportato.

Rilevamento delle sequenze di attacco nei gruppi di istanze Amazon EC2

GuardDuty è in grado di identificare le sequenze di attacco che interessano singole istanze o gruppi di istanze che condividono attributi comuni come gruppi di Auto Scaling, profili di istanze IAM, modelli di lancio, CloudFormation stack, AMI o ID VPC. Queste istanze possono presentare comportamenti sospetti come processi dannosi, connessioni a endpoint dannosi, crypto-mining o utilizzo anomalo delle credenziali delle istanze EC2.

L'individuazione della sequenza di attacco rileva i seguenti scenari di minaccia:

- Compromissione delle istanze che eseguono servizi vulnerabili
- Utilizzo delle credenziali dell'istanza Amazon EC2 ottenute tramite IMDS dall'esterno dell' AWS account a cui sono state emesse le credenziali
- Utilizzala come infrastruttura per attacchi quali proxy, scansione o denial of service
- Esecuzione non autorizzata di strumenti, malware o processi di cryptomining sospetti
- Comunicazione con endpoint sospetti

Extended Threat Detection aiuta a identificare queste minacce. GuardDuty rappresenta questi eventi correlati come un'unica rilevazione di gravità critica, denominata. `AttackSequence:EC2/CompromisedInstanceGroup`

Per migliorare le funzionalità di rilevamento di Extended Threat Detection for EC2, abilita il Runtime Monitoring. La combinazione di Foundational GuardDuty, che monitora l'attività di rete, CloudTrail e Runtime Monitoring, che osserva i comportamenti dei processi e le chiamate di sistema all'interno delle istanze, offre un rilevamento delle minacce più completo. Questo monitoraggio integrato consente di GuardDuty rilevare sequenze di attacco sofisticate come l'accesso non autorizzato tramite credenziali mal configurate, i tentativi di escalation dei privilegi e l'accesso non autorizzato a dati sensibili. Correlando questi diversi segnali, è GuardDuty possibile identificare modelli di attacco complessi che potrebbero non essere rilevati dai singoli rilevamenti e mappare il vettore di attacco completo.

Rilevamento esteso delle minacce nella console GuardDuty

Per impostazione predefinita, la pagina Extended Threat Detection nella GuardDuty console mostra lo stato come Abilitato. Con il rilevamento delle minacce di base, lo stato indica chi è in GuardDuty grado di rilevare una potenziale sequenza di attacco che coinvolge l'attività di individuazione dei privilegi IAM su Amazon APIs S3 e il rilevamento delle successive alterazioni del piano di controllo S3.

Utilizza i seguenti passaggi per accedere alla pagina Extended Threat Detection nella console: GuardDuty

1. È possibile aprire la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione a sinistra, scegli Extended Threat Detection.

Questa pagina fornisce dettagli sugli scenari di minaccia coperti da Extended Threat Detection.

3. Nella pagina Extended Threat Detection, visualizza la sezione Piani di protezione correlati. Se desideri abilitare piani di protezione dedicati per migliorare la copertura di rilevamento delle minacce nel tuo account, seleziona l'opzione Configura per quel piano di protezione.

Comprensione e gestione dei risultati della sequenza di attacco

I risultati della sequenza di attacco sono identici agli altri GuardDuty risultati del tuo account. Puoi visualizzarli nella pagina Findings della GuardDuty console. Per informazioni sulla visualizzazione dei risultati, vedere [Pagina dei risultati nella GuardDuty console](#).

Analogamente ad altri GuardDuty risultati, anche i risultati della sequenza di attacco vengono inviati automaticamente ad Amazon EventBridge. In base alle impostazioni, i risultati della sequenza di attacco vengono esportati anche in una destinazione di pubblicazione (bucket Amazon S3). Per impostare una nuova destinazione di pubblicazione o aggiornarne una esistente, consulta.

[Esportazione dei risultati generati su Amazon S3](#)

Risorse aggiuntive

Visualizza le seguenti sezioni per comprendere meglio le sequenze di attacco:

- Dopo aver appreso l'Extended Threat Detection e le sequenze di attacco, puoi generare esempi di tipi di ricerca delle sequenze di attacco seguendo i passaggi riportati di seguito. [Risultati di esempio](#)
- Ulteriori informazioni su [tipi di ricerca delle sequenze di attacco](#).
- Esamina i risultati ed esplora i dettagli associati [Dettagli del reperimento della sequenza di attacco](#) a.
- Assegna priorità e risolvi i tipi di ricerca delle sequenze di attacco seguendo i passaggi relativi alle risorse interessate associate in. [Correzioni degli esiti](#)

GuardDuty Protezione EKS

EKS Protection ti aiuta a rilevare potenziali rischi per la sicurezza nei cluster Amazon Elastic Kubernetes Service (Amazon EKS) nel tuo ambiente. AWS Ad esempio, ti aiuta a rilevare quando un attore non autenticato accede a un cluster EKS configurato in modo errato che tenta di raccogliere segreti o credenziali dal cluster. AWS EKS Protection utilizza i registri di controllo EKS per analizzare le attività di utenti e applicazioni.

Quando abiliti EKS Protection, avvia GuardDuty automaticamente il monitoraggio dei cluster Amazon EKS per potenziali minacce alla sicurezza. GuardDuty utilizza il proprio flusso indipendente per la raccolta e l'analisi [Registri di controllo EKS in EKS Protection](#): non è richiesta alcuna configurazione aggiuntiva.

Quando GuardDuty rileva una potenziale minaccia sulla base del monitoraggio del registro di controllo EKS, genera un risultato di sicurezza. Per informazioni sui tipi di risultati che GuardDuty possono essere generati quando si attiva EKS Protection, consulta [Tipi di risultati di protezione EKS](#).

Note

Per visualizzare i log di audit EKS nel tuo account (opzionale), puoi configurare la registrazione del piano di controllo di Amazon EKS per inviare i log di audit a Logs. CloudWatch Questa configurazione è separata da EKS Protection e non è richiesta per la funzionalità di monitoraggio della sicurezza in. GuardDuty

Prova gratuita di 30 giorni

- Quando abiliti la GuardDuty modalità « Account AWS in and» Regione AWS per la prima volta, ricevi una prova gratuita di 30 giorni. In questo caso, GuardDuty abiliterà anche EKS Protection, che è incluso nella prova gratuita di 30 giorni.
- Se stai già utilizzando GuardDuty e decidi di abilitare EKS Protection per la prima volta, il tuo account in questa regione riceverà una prova gratuita di 30 giorni per EKS Protection.
- Puoi scegliere di disabilitare EKS Protection in qualsiasi regione in qualsiasi momento.
- Durante la prova gratuita di 30 giorni, puoi ottenere una stima dei costi di utilizzo per quell'account e per quella regione. Al termine della prova gratuita di 30 giorni, GuardDuty non disabilita automaticamente EKS Protection. Il tuo account in questa regione inizierà a incorrere in costi di utilizzo. Per ulteriori informazioni, consulta [Monitoraggio dell'utilizzo e stima dei costi](#).

Quando disabiliti EKS Protection, interrompe GuardDuty immediatamente il monitoraggio e l'analisi dei log di audit EKS per le tue risorse Amazon EKS.

EKS Protection potrebbe non essere disponibile in tutti i paesi in Regioni AWS cui GuardDuty è disponibile. Per ulteriori informazioni, consulta [Disponibilità di funzionalità specifiche per ogni regione](#).

Note

EKS Runtime Monitoring è gestito come parte di Runtime Monitoring. Per ulteriori informazioni, consulta [GuardDuty monitoraggio del runtime](#).

Registri di controllo EKS in EKS Protection

I log di controllo EKS registrano le azioni sequenziali all'interno del cluster Amazon EKS, incluse le attività degli utenti, le applicazioni che utilizzano l'API Kubernetes e il piano di controllo. La registrazione di audit è un componente di tutti i cluster Kubernetes.

Per ulteriori informazioni, consultare [Auditing](#) nella documentazione Kubernetes.

Amazon EKS consente di importare i log di audit EKS come Amazon CloudWatch Logs tramite la funzionalità di registrazione del piano di [controllo EKS](#). GuardDuty non gestisce la registrazione del piano di controllo di Amazon EKS né rende accessibili i log di audit EKS nel tuo account se non li hai abilitati per Amazon EKS. Per gestire l'accesso e la conservazione dei log di audit EKS, devi configurare la funzionalità di registrazione del piano di controllo di Amazon EKS. Per ulteriori informazioni, consulta [Abilitazione e disabilitazione dei log del piano di controllo](#) nella Guida per l'utente di Amazon EKS.

Abilitazione della protezione EKS in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare la funzionalità EKS Protection; per gli account membro della propria organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Questo account GuardDuty amministratore delegato può scegliere di abilitare automaticamente EKS Protection per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta [Gestione di più account in Amazon](#). GuardDuty

Configurazione di EKS Audit Log Monitoring per un account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per configurare EKS Audit Log Monitoring per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Protezione EKS.
3. Nella scheda Configurazione, puoi visualizzare lo stato di configurazione attuale del monitoraggio dei log di audit EKS nella sezione corrispondente. Per aggiornare la configurazione per l'account GuardDuty amministratore delegato, scegliete Modifica nel riquadro EKS Audit Log Monitoring.
4. Esegui una delle seguenti operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Scegli Save (Salva).

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Scegli Save (Salva).

API/CLI

Esegui l'operazione API [updateDetector](#) utilizzando il tuo ID rilevatore regionale e impostando il name dell'oggetto features su EKS_AUDIT_LOGS e lo status su ENABLED o DISABLED.

Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

È possibile abilitare o disabilitare EKS Audit Log Monitoring eseguendo il seguente AWS CLI comando. Assicurati di utilizzare un account di GuardDuty amministratore delegato valido *detector ID*.

 Note

Il codice di esempio seguente abilita il monitoraggio dei log di audit EKS. Assicurati di sostituirlo *12abc34d567e8fa901bc2d34e56789f0* con l'account `detector-id` dell' GuardDuty amministratore delegato e *5555555555* con l'account Account AWS dell'amministratore delegato GuardDuty .

Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Per disabilitare il monitoraggio dei log di audit EKS, sostituisci `ENABLED` con `DISABLED`.

Abilitare automaticamente il monitoraggio dei log di audit EKS per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio dei log di audit EKS per account membri esistenti dell'organizzazione.

Console

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

Utilizzando la pagina Protezione EKS

1. Nel riquadro di navigazione, scegli Protezione EKS.
2. Nella scheda Configurazione, puoi visualizzare lo stato attuale del monitoraggio dei log di audit EKS per gli account membri attivi dell'organizzazione.

Per aggiornare la configurazione del monitoraggio dei log di audit EKS, scegli Modifica.

3. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente il monitoraggio dei log di audit EKS per gli account dell'organizzazione esistenti e per quelli nuovi.
4. Scegli Save (Salva).

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio dei log di audit EKS.
4. Scegli Save (Salva).

Se non puoi utilizzare l'opzione Abilita per tutti gli account e desideri personalizzare la configurazione del monitoraggio dei log di audit EKS per account specifici dell'organizzazione, consulta [Abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per gli account membri](#).

API/CLI

- Per abilitare o disabilitare in modo selettivo EKS Audit Log Monitoring per i vostri account membri, eseguite l'operazione [updateMemberDetectors](#) API utilizzando le vostre *detector ID*.

- L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per un singolo account membro. Per disabilitarla, sostituisci ENABLED con DISABLED.

Per trovare le detectorId impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui l'[ListDetectorsAPI](#).

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

Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare il monitoraggio dei log di audit EKS per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio dei log di audit EKS per tutti gli account membri attivi esistenti dell'organizzazione.

Console

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, scegli Protezione EKS.
3. Nella pagina EKS Protection, è possibile visualizzare lo stato corrente della configurazione della scansione GuardDutyantimalware avviata. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Save (Salva).

API/CLI

- Per abilitare o disabilitare in modo selettivo EKS Audit Log Monitoring per gli account dei membri, esegui l'operazione [updateMemberDetectors](#) API utilizzando la tua *detector ID*.
- L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per un singolo account membro. Per disabilitarla, sostituisci ENABLED con DISABLED.

Per trovare le detectorId impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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



Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente il monitoraggio dei log di audit EKS per i nuovi account membri

Gli account membro appena aggiunti devono essere abilitati GuardDuty prima di selezionare la configurazione della scansione GuardDuty antimalware avviata. Gli account membri gestiti su invito possono configurare manualmente la scansione antimalware GuardDuty avviata per i propri account. Per ulteriori informazioni, consulta [Step 3 - Accept an invitation](#).

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio dei log di audit EKS per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare EKS Audit Log Monitoring per i nuovi account membro di un'organizzazione, utilizzando la pagina EKS Audit Log Monitoring o Accounts.

Per abilitare automaticamente il monitoraggio dei log di audit EKS per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

- Utilizzando la pagina Protezione EKS:
 1. Nel riquadro di navigazione, scegli Protezione EKS.
 2. Nella pagina Protezione EKS, scegli Modifica nel monitoraggio dei log di audit EKS.
 3. Scegli Configura gli account manualmente.
 4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica del monitoraggio dei log di audit EKS per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
 5. Scegli Save (Salva).
- Utilizzando la pagina Account:
 1. Dal riquadro di navigazione, selezionare Accounts (Account).
 2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
 3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio dei log di audit EKS.
 4. Scegli Save (Salva).

API/CLI

- Per abilitare o disabilitare in modo selettivo EKS Audit Log Monitoring per i nuovi account, esegui l'operazione [UpdateOrganizationConfiguration](#) API utilizzando la tua *detector ID*

- L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per i nuovi membri che entrano a far parte dell'organizzazione. Puoi anche passare un elenco di account IDs separati da uno spazio.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui l'[ListDetectors](#) API.

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

Abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per gli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare il monitoraggio dei log di audit EKS per account membri selettivi dell'organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

Nella pagina Account, consulta la colonna Monitoraggio dei log di audit EKS per visualizzare lo stato del tuo account membro.

3. Abilitare o disabilitare il monitoraggio dei log di audit EKS

Seleziona un account da configurare per il monitoraggio dei log di audit EKS. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli Monitoraggio dei log di audit EKS, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo EKS Audit Log Monitoring per i vostri account membri, richiamate l'operazione [updateMemberDetectors](#) API utilizzando la vostra *detector ID*

L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per un singolo account membro. Per disabilitarla, sostituisci ENABLED con DISABLED. Puoi anche passare un elenco di account IDs separati da uno spazio.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

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

Attivazione di EKS Protection per un account autonomo

A un account indipendente spetta la decisione di abilitare o disabilitare un piano di protezione nel proprio AWS account in una regione specifica.

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non ti riguarda. Per informazioni sulla gestione di più account, consulta [Abilitazione della protezione EKS in ambienti con più account](#).

Dopo aver abilitato EKS Protection, GuardDuty inizierai a monitorare i log di controllo EKS per i cluster Amazon EKS nel tuo account.

Scegli il metodo di accesso preferito per abilitare EKS Protection nel tuo account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Dal selettore della regione nell'angolo in alto a destra, seleziona una regione in cui desideri abilitare la protezione EKS.
3. Nel riquadro di navigazione, scegli Protezione EKS.
4. La pagina EKS Protection fornisce lo stato attuale di EKS Protection per il tuo account. Scegli Abilita per abilitare EKS Protection.
5. Scegli Conferma per salvare la selezione.

API/CLI

- Esegui l'operazione [updateDetector](#) API utilizzando l'ID del rilevatore regionale dell'account GuardDuty amministratore delegato e passando il nome dell'feature soggetto EKS_AUDIT_LOGS e lo status as. ENABLED

In alternativa, puoi anche abilitare EKS Protection eseguendo il comando a AWS CLI . Esegui il comando seguente e sostituiscilo `12abc34d567e8fa901bc2d34e56789f0` con l'ID del rilevatore del tuo account e `us-east-1` con la regione in cui desideri abilitare EKS Protection.

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

GuardDuty Protezione S3

S3 Protection ti aiuta a rilevare potenziali rischi per la sicurezza dei dati, come l'esfiltrazione e la distruzione dei dati, nei bucket Amazon Simple Storage Service (Amazon S3). GuardDuty monitora gli eventi AWS CloudTrail relativi ai dati per Amazon S3, che includono operazioni API a livello di oggetto per identificare questi rischi in tutti i bucket Amazon S3 del tuo account.

Quando GuardDuty rileva una potenziale minaccia basata sul monitoraggio degli eventi relativi ai dati di S3, genera una rilevazione di sicurezza. Per informazioni sui tipi di risultati che GuardDuty possono essere generati quando abiliti S3 Protection, consulta [GuardDuty S3 Tipi di risultati di protezione](#)

Per impostazione predefinita, il rilevamento delle minacce di base include [AWS CloudTrail eventi di gestione](#) il monitoraggio per identificare potenziali minacce nelle risorse Amazon S3. Questa fonte di dati è diversa dagli eventi AWS CloudTrail relativi ai dati di S3 in quanto entrambi monitorano diversi tipi di attività nel tuo ambiente.

Puoi abilitare S3 Protection in un account in qualsiasi regione in cui GuardDuty [supporta questa funzionalità](#). Questo ti aiuterà a monitorare gli eventi CloudTrail relativi ai dati per S3 in quell'account e nella regione. Dopo aver abilitato S3 Protection, GuardDuty sarai in grado di monitorare completamente i tuoi bucket Amazon S3 e generare rilevazioni di accessi sospetti ai dati archiviati nei tuoi bucket S3.

Per utilizzare S3 Protection, non è necessario abilitare o configurare in modo esplicito la registrazione degli eventi di dati S3. AWS CloudTrail

Prova gratuita di 30 giorni

L'elenco seguente spiega come potrebbe funzionare la prova gratuita di 30 giorni per il tuo account:

- Quando la attivi GuardDuty Account AWS in una nuova regione per la prima volta, ricevi una prova gratuita di 30 giorni. In questo caso, GuardDuty abiliterà anche S3 Protection, incluso nella versione di prova gratuita.
- Se utilizzi già S3 Protection GuardDuty e decidi di abilitare S3 Protection per la prima volta, il tuo account in questa regione riceverà una prova gratuita di 30 giorni per S3 Protection.
- Puoi scegliere di disabilitare S3 Protection in qualsiasi regione e in qualsiasi momento.
- Durante la prova gratuita di 30 giorni, puoi ottenere una stima dei costi di utilizzo per quell'account e per quella regione. Al termine della prova gratuita di 30 giorni, S3 Protection non viene disabilitato automaticamente. Il tuo account in questa regione inizierà a incorrere in costi

di utilizzo. Per ulteriori informazioni, consulta [Monitoraggio GuardDuty dell'utilizzo e stima dei costi](#).

AWS CloudTrail eventi relativi ai dati per S3

Gli eventi di dati, anche conosciuti come operazioni del piano dati, forniscono informazioni dettagliate sulle operazioni eseguite su una risorsa o al suo interno e sono spesso attività che interessano volumi elevati di dati.

Di seguito sono riportati alcuni esempi di eventi CloudTrail relativi ai dati per S3 che è GuardDuty possibile monitorare:

- Operazioni API `GetObject`
- Operazioni API `PutObject`
- Operazioni API `ListObjects`
- Operazioni API `DeleteObject`

Per ulteriori informazioni al riguardo APIs, consulta [Amazon Simple Storage Service API Reference](#).

In che modo GuardDuty utilizza gli eventi CloudTrail relativi ai dati per S3

Quando abiliti S3 Protection, GuardDuty inizia ad analizzare gli eventi CloudTrail relativi ai dati per S3 provenienti da tutti i bucket S3 e li monitora per rilevare eventuali attività dannose e sospette. Per ulteriori informazioni, consulta [AWS CloudTrail eventi di gestione](#).

Quando un utente non autenticato accede a un oggetto S3, significa che l'oggetto S3 è accessibile pubblicamente. Pertanto, GuardDuty non elabora tali richieste. GuardDuty elabora le richieste fatte agli oggetti S3 utilizzando credenziali IAM (AWS Identity and Access Management) o AWS STS (AWS Security Token Service) valide.

Nota

Dopo aver abilitato S3 Protection, GuardDuty monitora gli eventi relativi ai dati provenienti da quei bucket Amazon S3 che risiedono nella stessa regione in cui hai abilitato. GuardDuty

Se disabiliti S3 Protection nel tuo account in una regione specifica, GuardDuty interrompe il monitoraggio degli eventi di dati S3 dei dati archiviati nei bucket S3. GuardDuty non genererà più i tipi di risultati di S3 Protection per il tuo account in quella regione.

GuardDuty utilizzo di eventi CloudTrail relativi ai dati per S3 per le sequenze di attacco

[GuardDuty Rilevamento esteso delle minacce](#) rileva sequenze di attacco in più fasi che abbracciano fonti di dati, AWS risorse e cronologia fondamentali, in un account. Quando GuardDuty rileva una sequenza di eventi indicativa di un'attività sospetta recente o in corso nel tuo account, genera la relativa sequenza di attacco. GuardDuty

Per impostazione predefinita, quando abiliti GuardDuty, anche Extended Threat Detection viene abilitato nel tuo account. Questa funzionalità copre lo scenario di minaccia associato agli eventi di CloudTrail gestione senza costi aggiuntivi. Tuttavia, per utilizzare Extended Threat Detection al massimo delle sue potenzialità, GuardDuty consigliamo di abilitare S3 Protection per coprire gli scenari di minaccia associati agli eventi CloudTrail relativi ai dati per S3.

Dopo aver abilitato S3 Protection, GuardDuty coprirà automaticamente gli scenari di minaccia della sequenza di attacco, come la compromissione o la distruzione dei dati, in cui potrebbero essere coinvolte le tue risorse Amazon S3.

Abilitazione della protezione S3 in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di configurare (abilitare o disabilitare) S3 Protection per gli account dei membri della propria organizzazione. AWS GuardDutyGli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. L'account GuardDuty amministratore delegato può scegliere di abilitare automaticamente S3 Protection su tutti gli account, solo sui nuovi account o su nessun account dell'organizzazione. Per ulteriori informazioni, consulta [Gestione degli account con AWS Organizations](#).

Abilitazione di S3 Protection per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per abilitare S3 Protection per l'account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guarddduty/>
2. Nel riquadro di navigazione, scegli Protezione S3.
3. Nella pagina Protezione S3, scegli Modifica.
4. Esegui una delle seguenti operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Scegli Save (Salva).

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Scegli Save (Salva).

API/CLI

Esegui [updateDetector](#) utilizzando l'ID del rilevatore dell'account GuardDuty amministratore delegato per la regione corrente e passando l'featuresoggetto di tanto in name tantoS3_DATA_EVENTS. status ENABLED

In alternativa, puoi configurare S3 Protection utilizzando. AWS Command Line Interface Esegui il comando seguente e assicurati di sostituirlo **12abc34d567e8fa901bc2d34e56789f0** con l'ID del rilevatore dell'account GuardDuty amministratore delegato per la regione corrente.

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guarddduty/console> o esegui l'[ListDetectors](#)API.

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

Abilitare automaticamente la Protezione S3 per tutti gli account membri dell'organizzazione

Scegli il metodo di accesso preferito per abilitare S3 Protection per l' GuardDuty account amministratore delegato.

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Accedi utilizzando il tuo account amministratore.

2. Esegui una delle seguenti operazioni:

Utilizzando la pagina Protezione S3

1. Nel riquadro di navigazione, scegli Protezione S3.
2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente la Protezione S3 per gli account dell'organizzazione esistenti e per quelli nuovi.
3. Scegli Save (Salva).

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Protezione S3.
4. Scegli Save (Salva).

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta [Abilita selettivamente S3 Protection negli account dei membri](#).

API/CLI

- Per abilitare in modo selettivo S3 Protection per i tuoi account membro, richiama l'operazione [updateMemberDetectors](#) API utilizzando la tua *detector ID*
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Assicurati di sostituirlo *12abc34d567e8fa901bc2d34e56789f0* con `detector-id` l'GuardDuty account amministratore delegato e *111122223333*

Per trovare l'`detectorId` account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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



Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare la Protezione S3 per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare la Protezione S3 per tutti gli account membri attivi esistenti dell'organizzazione.

Console

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, scegli Protezione S3.
3. Nella pagina Protezione S3, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.

4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare in modo selettivo S3 Protection per i tuoi account membro, richiama l'operazione [updateMemberDetectors](#) API utilizzando le tue *detector ID*
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Assicurati di sostituirlo *12abc34d567e8fa901bc2d34e56789f0* con `detector-id` l'GuardDuty account amministratore delegato e *111122223333*

Per trovare l'`detectorId` account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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



Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente la Protezione S3 per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare la Protezione S3 per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare nuovi account membro in un'organizzazione tramite la console, utilizzando la pagina S3 Protection o Account.

Per abilitare automaticamente la Protezione S3 per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:
 - Utilizzando la pagina Protezione S3:
 1. Nel riquadro di navigazione, scegli Protezione S3.
 2. Nella pagina Protezione S3, scegli Modifica.
 3. Scegli Configura gli account manualmente.
 4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione S3 per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
 5. Scegli Save (Salva).
 - Utilizzando la pagina Account:
 1. Dal riquadro di navigazione, selezionare Accounts (Account).
 2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
 3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Protezione S3.
 4. Scegli Save (Salva).

API/CLI

- Per abilitare selettivamente S3 Protection per i tuoi account membro, richiama l'operazione [UpdateOrganizationConfiguration](#) API utilizzando la tua. *detector ID*
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Imposta le preferenze in modo da abilitare o disabilitare automaticamente il piano di protezione in una determinata regione per i nuovi account che entrano a far parte dell'organizzazione (NEW), per tutti gli account (ALL) o per nessuno degli account dell'organizzazione (NONE). [Per ulteriori informazioni, consulta Membri. autoEnableOrganization](#) In base alle tue preferenze, potrebbe essere necessario sostituire NEW con ALL o NONE.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita selettivamente S3 Protection negli account dei membri

Scegli il tuo metodo di accesso preferito per abilitare in modo selettivo S3 Protection per gli account dei membri.

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

Nella pagina Account, consulta la colonna Protezione S3 per visualizzare lo stato del tuo account membro.

3. Per abilitare selettivamente S3 Protection

Seleziona l'account per il quale desideri abilitare S3 Protection. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli S3Pro, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare in modo selettivo S3 Protection per i tuoi account membro, esegui l'operazione [updateMemberDetectors](#) API utilizzando il tuo ID di rilevamento. L'esempio seguente mostra come

abilitare la Protezione S3 per un singolo account membro. Per disabilitarla, sostituisci `true` con `false`.

Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'API.

[ListDetectors](#)

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

 Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

 Note

Se utilizzi script per aggiungere nuovi account nei quali desideri disabilitare la Protezione S3, puoi modificare l'operazione API [createDetector](#) con l'oggetto `dataSources` facoltativo, come descritto in questo argomento.

Attivazione di S3 Protection per un account autonomo

A un account autonomo spetta la decisione di abilitare o disabilitare un piano di protezione in uno specifico account Account AWS . Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione della protezione S3 in ambienti con più account](#).

Dopo aver abilitato S3 Protection, GuardDuty inizierà a monitorare gli eventi AWS CloudTrail relativi ai dati per i bucket S3 presenti nel tuo account.

Scegli il metodo di accesso che preferisci per configurare la Protezione S3 per un account autonomo.

Console

1. Accedi a Console di gestione AWS e apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Dal selettore della regione nell'angolo in alto a destra, seleziona una regione in cui desideri abilitare la protezione S3.
3. Nel riquadro di navigazione, scegli Protezione S3.
4. La pagina Protezione S3 fornisce lo stato attuale della Protezione S3 per il tuo account. Scegli Abilita o Disabilita per abilitare o disabilitare in qualsiasi momento la Protezione S3.
5. Scegli Conferma per confermare la selezione.

API/CLI

Esegui [updateDetector](#) utilizzando l'ID del rilevatore valido per la regione corrente e passando l'featuresoggetto name come S3_DATA_EVENTS impostato per abilitare rispettivamente la protezione S3ENABLED.

Note

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#)API.

In alternativa, puoi usare AWS Command Line Interface. Per abilitare S3 Protection, esegui il comando seguente e sostituiscilo **12abc34d567e8fa901bc2d34e56789f0** con l'ID del rilevatore del tuo account e **us-east-1** con la regione in cui desideri abilitare S3 Protection.

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

GuardDuty monitoraggio del runtime

Runtime Monitoring osserva e analizza gli eventi a livello di sistema operativo, di rete e di file per aiutarti a rilevare potenziali minacce in carichi di AWS lavoro specifici del tuo ambiente.

AWS Risorse supportate in Runtime Monitoring: inizialmente GuardDuty aveva rilasciato Runtime Monitoring per supportare solo le risorse Amazon Elastic Kubernetes Service (Amazon EKS). Ora puoi utilizzare la funzionalità Runtime Monitoring per rilevare le minacce anche per le tue risorse AWS Fargate Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Compute Cloud (Amazon EC2).

GuardDuty non supporta i cluster Amazon EKS in esecuzione su AWS Fargate.

In questo documento e in altre sezioni relative al Runtime Monitoring, GuardDuty utilizza la terminologia del tipo di risorsa per fare riferimento alle risorse Amazon EKS, Fargate, Amazon ECS e Amazon EC2.

Runtime Monitoring utilizza un agente GuardDuty di sicurezza che aggiunge visibilità al comportamento di runtime, come l'accesso ai file, l'esecuzione dei processi, gli argomenti della riga di comando e le connessioni di rete. Per ogni tipo di risorsa che desideri monitorare per rilevare potenziali minacce, puoi gestire l'agente di sicurezza per quel tipo di risorsa specifico automaticamente o manualmente (ad eccezione di Fargate (solo Amazon ECS)). La gestione automatica del security agent significa che autorizzi l'installazione e l'aggiornamento del security agent GuardDuty per tuo conto. D'altra parte, quando gestisci manualmente il security agent per le tue risorse, sei responsabile dell'installazione e dell'aggiornamento del security agent, se necessario.

Grazie a questa funzionalità estesa, GuardDuty può aiutarvi a identificare e rispondere a potenziali minacce che possono colpire le applicazioni e i dati in esecuzione nei singoli carichi di lavoro e istanze. Ad esempio, una minaccia può iniziare compromettendo un singolo container che esegue un'applicazione Web vulnerabile. Questa applicazione Web potrebbe disporre delle autorizzazioni di accesso ai container e ai carichi di lavoro sottostanti. In questo scenario, le credenziali configurate in modo errato potrebbero portare a un accesso più ampio all'account e ai dati archiviati al suo interno.

Analizzando gli eventi di runtime dei singoli container e carichi di lavoro, GuardDuty può potenzialmente identificare la compromissione di un container e delle relative AWS credenziali in una fase iniziale e rilevare tentativi di aumentare i privilegi, richieste API sospette e accessi malevoli ai dati presenti nell'ambiente.

Indice

- [Come funziona](#)
- [Come funziona la versione di prova gratuita di 30 giorni in Runtime Monitoring](#)
- [Prerequisiti per abilitare il monitoraggio del runtime](#)
- [Abilitazione del monitoraggio del GuardDuty runtime](#)
- [Gestione degli agenti GuardDuty di sicurezza](#)
- [Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi](#)
- [Configurazione del monitoraggio della CPU e della memoria](#)
- [Utilizzo di un VPC condiviso con Runtime Monitoring](#)
- [Utilizzo di Infrastructure as Code \(IaC\) con agenti di sicurezza automatizzati GuardDuty](#)
- [Tipi di eventi di runtime raccolti che GuardDuty utilizzano](#)
- [Agente di hosting del repository Amazon ECR GuardDuty](#)
- [Due agenti di sicurezza sullo stesso host sottostante](#)
- [Monitoraggio del runtime EKS in GuardDuty](#)
- [GuardDuty versioni di rilascio di Security Agent](#)
- [Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring](#)

Come funziona

Per utilizzare Runtime Monitoring, è necessario abilitare il Runtime Monitoring e quindi gestire il security agent. GuardDuty L'elenco seguente illustra questo processo in due fasi:

1. Abilita il monitoraggio del runtime per il tuo account in modo che GuardDuty possa accettare gli eventi di runtime che riceve dalle tue istanze Amazon EC2, dai cluster Amazon ECS e dai carichi di lavoro Amazon EKS.
2. Gestisci GuardDuty l'agente per le singole risorse di cui desideri monitorare il comportamento di runtime. In base al tipo di risorsa, puoi scegliere di:
 - Utilizza la configurazione automatizzata degli agenti, che GuardDuty gestisce la distribuzione degli agenti e automaticamente un endpoint Amazon Virtual Private Cloud (Amazon VPC).
 - Installa l'agente manualmente, il che richiede la creazione dell'endpoint VPC come prerequisito.

L'agente di sicurezza utilizza l'endpoint VPC per fornire eventi GuardDuty, garantendo che i dati rimangano all'interno della rete. AWS Questo approccio migliora la sicurezza e consente di GuardDuty monitorare e analizzare il comportamento di runtime tra le tue risorse (Amazon EKS,

Amazon EC2 AWS Fargate e -Amazon ECS). GuardDuty utilizza i [ruoli di identità dell'istanza](#) che autenticano il security agent per ogni tipo di risorsa per inviare gli eventi di runtime associati all'endpoint VPC.

 Note

GuardDuty non rende gli eventi di runtime accessibili all'utente.

Quando gestisci l'agente di sicurezza (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring for EC2 e GuardDuty viene attualmente distribuito su un'istanza Amazon EC2 e riceve i dati [Tipi di eventi di runtime raccolti](#) da questa istanza, non GuardDuty ti verrà addebitato alcun costo per Account AWS l'analisi dei log di flusso VPC da questa istanza Amazon EC2. Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

I seguenti argomenti spiegano come l'attivazione del Runtime Monitoring e la gestione del GuardDuty Security Agent funzionino in modo diverso per ogni tipo di risorsa.

Indice

- [Come funziona il monitoraggio del runtime con i cluster Amazon EKS](#)
- [Come funziona il monitoraggio del runtime con le istanze Amazon EC2](#)
- [Come funziona il monitoraggio del runtime con Fargate \(solo Amazon ECS\)](#)
- [Dopo aver abilitato il monitoraggio del runtime](#)

Come funziona il monitoraggio del runtime con i cluster Amazon EKS

Runtime Monitoring utilizza un [componente aggiuntivo EKS aws-guardduty-agent](#), chiamato anche agente di GuardDuty sicurezza. Dopo che l'agente GuardDuty di sicurezza è stato distribuito sui cluster EKS, GuardDuty è in grado di ricevere eventi di runtime per questi cluster EKS.

 Note

Runtime Monitoring supporta i cluster Amazon EKS in esecuzione su istanze Amazon EC2 e Amazon EKS Auto Mode.

Runtime Monitoring non supporta i cluster Amazon EKS con Amazon EKS Hybrid Nodes e quelli in AWS Fargate esecuzione.

Per informazioni su queste funzionalità di Amazon EKS, consulta [Cos'è Amazon EKS?](#) nella Guida per l'utente di Amazon EKS.

Puoi monitorare gli eventi di runtime dei tuoi cluster Amazon EKS a livello di account o di cluster. Puoi gestire l'agente GuardDuty di sicurezza solo per i cluster Amazon EKS che desideri monitorare per il rilevamento delle minacce. Puoi gestire l'agente GuardDuty di sicurezza manualmente o consentendone la gestione GuardDuty per tuo conto, utilizzando la configurazione automatizzata dell'agente.

Quando utilizzi l'approccio di configurazione automatizzata degli agenti GuardDuty per consentire di gestire l'implementazione del security agent per tuo conto, questo creerà automaticamente un endpoint Amazon Virtual Private Cloud (Amazon VPC). Il security agent fornisce gli eventi di runtime GuardDuty utilizzando questo endpoint Amazon VPC.

Oltre all'endpoint VPC, crea GuardDuty anche un nuovo gruppo di sicurezza. Le regole in entrata (ingresso) controllano il traffico autorizzato a raggiungere le risorse associate al gruppo di sicurezza. GuardDuty aggiunge regole in entrata che corrispondono all'intervallo CIDR VPC per la risorsa e si adatta anche quando l'intervallo CIDR cambia. Per ulteriori informazioni, consulta la [gamma VPC CIDR](#) nella Amazon VPC User Guide.

Note

- Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint VPC.
- Utilizzo di un VPC centralizzato con agente automatizzato: quando GuardDuty utilizzi la configurazione automatica degli agenti per un tipo di risorsa GuardDuty, creerà un endpoint VPC per tuo conto per tutti. VPCs Ciò include il VPC e lo spoke centralizzati. VPCs GuardDuty non supporta la creazione di un endpoint VPC solo per il VPC centralizzato. Per ulteriori informazioni sul funzionamento del VPC centralizzato, consulta [Interface VPC endpoint nel Whitepaper - Creazione di un'infrastruttura di AWS rete multi-VPC](#) scalabile e sicura. AWS

Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS

Prima del 13 settembre 2023, era possibile configurare GuardDuty la gestione del security agent a livello di account. Questo comportamento indicava che, per impostazione predefinita, GuardDuty

gestirà il security agent su tutti i cluster EKS che appartengono a un Account AWS. Ora GuardDuty fornisce una funzionalità granulare per aiutarvi a scegliere i cluster EKS in cui desiderate gestire l'agente GuardDuty di sicurezza.

Se scegli [Gestisci l'agente GuardDuty di sicurezza manualmente](#), puoi comunque selezionare i cluster EKS che desideri monitorare. Tuttavia, per gestire l'agente manualmente, la creazione di un endpoint Amazon VPC per il tuo Account AWS è un prerequisito.

Note

Indipendentemente dall'approccio utilizzato per gestire l'agente di GuardDuty sicurezza, EKS Runtime Monitoring è sempre abilitato a livello di account.

Argomenti

- [Gestisci l'agente di sicurezza tramite GuardDuty](#)
- [Gestisci l'agente GuardDuty di sicurezza manualmente](#)

Gestisci l'agente di sicurezza tramite GuardDuty

GuardDuty implementa e gestisce il security agent per tuo conto. Puoi monitorare i cluster EKS nel tuo account in qualsiasi momento utilizzando uno degli approcci seguenti.

Argomenti

- [Monitora tutti i cluster EKS](#)
- [Esclude i cluster EKS selettivi](#)
- [Includi cluster EKS selettivi](#)

Monitora tutti i cluster EKS

Utilizza questo approccio quando desideri GuardDuty implementare e gestire l'agente di sicurezza per tutti i cluster EKS del tuo account. Per impostazione predefinita, GuardDuty implementerà il security agent anche su un cluster EKS potenzialmente nuovo creato nel tuo account.

Impatto dell'utilizzo di questo approccio

- GuardDuty crea un endpoint Amazon Virtual Private Cloud (Amazon VPC) attraverso il quale il GuardDuty security agent consegna gli eventi di runtime. GuardDuty Non sono previsti costi

aggiuntivi per la creazione dell'endpoint Amazon VPC quando si gestisce il security agent tramite GuardDuty

- È necessario che il nodo di lavoro disponga di un percorso di rete valido verso un endpoint guardduty-data VPC attivo. GuardDuty implementa il security agent sui tuoi cluster EKS. Amazon Elastic Kubernetes Service (Amazon EKS) coordinerà l'implementazione dell'agente di sicurezza sui nodi all'interno dei cluster EKS.
- In base alla disponibilità IP, GuardDuty seleziona la sottorete per creare un endpoint VPC. Se utilizzi topologie di rete avanzate, devi verificare che la connettività sia possibile.

Esclude i cluster EKS selettivi

Utilizza questo approccio quando desideri gestire l'agente GuardDuty di sicurezza per tutti i cluster EKS del tuo account ma escludere i cluster EKS selettivi. Questo metodo utilizza un approccio¹ basato su tag in cui puoi assegnare tag ai cluster EKS per i quali non desideri ricevere gli eventi di runtime. La coppia chiave-valore del tag predefinito deve essere `GuardDutyManaged=false`.

Impatto dell'utilizzo di questo approccio

Questo approccio richiede l'attivazione della gestione automatica degli GuardDuty agenti solo dopo aver aggiunto tag ai cluster EKS che si desidera escludere dal monitoraggio.

Pertanto, [Gestisci l'agente di sicurezza tramite GuardDuty](#) incide anche su questo approccio. Quando aggiungi tag prima di abilitare la gestione automatica degli GuardDuty agenti, non GuardDuty distribuirà né gestirà l'agente di sicurezza per i cluster EKS esclusi dal monitoraggio.

Considerazioni

- È necessario aggiungere la coppia chiave-valore del tag come `GuardDutyManaged=false` per i cluster EKS selettivi prima di abilitare la configurazione automatizzata dell'agente, altrimenti, l'agente di GuardDuty sicurezza verrà distribuito su tutti i cluster EKS fino a quando non si utilizza il tag.
- È necessario fare in modo che i tag vengano modificati solo da identità affidabili.

Important

Gestisci le autorizzazioni per modificare il valore del tag `GuardDutyManaged` per il cluster EKS utilizzando le policy di controllo dei servizi o le policy IAM. Per

ulteriori informazioni, consulta [Service control policies \(SCPs\)](#) nella Guida per l'AWS Organizations utente o [Control access to AWS resources](#) nella IAM User Guide.

- Assicurati di aggiungere la coppia chiave-valore `GuardDutyManaged-false` al momento della creazione di un cluster EKS potenzialmente nuovo che non desideri monitorare.
- La considerazione specificata per [Monitora tutti i cluster EKS](#) vale anche per questo approccio.

Includi cluster EKS selettivi

Utilizza questo approccio quando desideri GuardDuty distribuire e gestire gli aggiornamenti del security agent solo per i cluster EKS selettivi del tuo account. Questo metodo utilizza un approccio¹ basato su tag in cui puoi assegnare tag al cluster EKS per il quale desideri ricevere gli eventi di runtime.

Impatto dell'utilizzo di questo approccio

- Utilizzando i tag di inclusione, GuardDuty implementerà e gestirà automaticamente il security agent solo per i cluster EKS selettivi contrassegnati con `GuardDutyManaged - true` come coppia chiave-valore.
- L'utilizzo di questo approccio avrà lo stesso impatto specificato per [Monitora tutti i cluster EKS](#).

Considerazioni

- Se il valore del tag `GuardDutyManaged` non è impostato su `true`, il tag di inclusione non funzionerà come previsto e ciò potrebbe influire sul monitoraggio del cluster EKS.
- Per garantire il monitoraggio dei cluster EKS selettivi, è necessario fare in modo che i tag vengano modificati solo da identità affidabili.

Important

Gestisci le autorizzazioni per modificare il valore del tag `GuardDutyManaged` per il cluster EKS utilizzando le policy di controllo dei servizi o le policy IAM. Per ulteriori informazioni, consulta [Service control policies \(SCPs\)](#) nella Guida per l'AWS Organizations utente o [Control access to AWS resources](#) nella IAM User Guide.

- Assicurati di aggiungere la coppia chiave-valore `GuardDutyManaged-false` al momento della creazione di un cluster EKS potenzialmente nuovo che non desideri monitorare.
- La considerazione specificata per [Monitora tutti i cluster EKS](#) vale anche per questo approccio.

¹ Per ulteriori informazioni su come assegnare tag ai cluster EKS selettivi, consulta [Assegnazione di tag alle risorse Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Gestisci l'agente GuardDuty di sicurezza manualmente

Utilizza questo approccio quando desideri implementare e gestire manualmente il GuardDuty security agent su tutti i cluster EKS. Assicurati che il monitoraggio del runtime EKS sia abilitato per i tuoi account. L'agente GuardDuty di sicurezza potrebbe non funzionare come previsto se non abiliti EKS Runtime Monitoring.

Impatto dell'utilizzo di questo approccio

Dovrete coordinare l'implementazione del GuardDuty security agent all'interno dei cluster EKS su tutti gli account e Regioni AWS laddove questa funzionalità sia disponibile. Sarà inoltre necessario aggiornare la versione dell'agente quando viene GuardDuty rilasciata. Per ulteriori informazioni sulle versioni degli agenti per EKS, consulta [GuardDuty versioni degli agenti di sicurezza per le risorse Amazon EKS](#).

Considerazioni

È necessario supportare un flusso di dati sicuro monitorando e risolvendo al contempo le lacune di copertura man mano che nuovi cluster e carichi di lavoro vengono continuamente implementati.

Come funziona il monitoraggio del runtime con le istanze Amazon EC2

Le tue istanze Amazon EC2 possono eseguire diversi tipi di applicazioni e carichi di lavoro nel tuo ambiente. AWS Quando abiliti il monitoraggio del runtime e gestisci l'agente GuardDuty di sicurezza, ti GuardDuty aiuta a rilevare le minacce nelle istanze Amazon EC2 esistenti e in quelle potenzialmente nuove. Questa funzionalità supporta anche le istanze Amazon EC2 gestite da Amazon ECS. Per ulteriori informazioni, consulta il supporto delle [istanze gestite](#) in Guarddduty.

Note

Il monitoraggio del runtime non supporta le applicazioni in esecuzione su [Amazon ECS Managed Instances](#).

L'abilitazione del monitoraggio del runtime consente GuardDuty di utilizzare gli eventi di runtime dei processi attualmente in esecuzione e dei nuovi processi all'interno delle istanze Amazon EC2.

GuardDuty richiede un agente di sicurezza a cui inviare gli eventi di runtime dall'istanza EC2 a GuardDuty

Per le istanze Amazon EC2, il GuardDuty security agent opera a livello di istanza. Puoi decidere se monitorare tutte le istanze Amazon EC2 o solo alcune istanze Amazon EC2 nel tuo account. Se desideri gestire istanze selettive, l'agente di sicurezza è necessario solo per queste istanze.

GuardDuty può anche utilizzare eventi di runtime da nuove attività e attività esistenti in esecuzione in istanze Amazon EC2 all'interno di cluster Amazon ECS.

Per installare l'agente GuardDuty di sicurezza, Runtime Monitoring offre le seguenti due opzioni:

- [Utilizza la configurazione automatica degli agenti \(scelta consigliata\)](#), oppure
- [Gestisci l'agente di sicurezza manualmente](#)

Utilizza la configurazione automatica degli agenti tramite GuardDuty (consigliato)

Utilizza la configurazione automatizzata dell'agente che consente GuardDuty di installare l'agente di sicurezza sulle tue istanze Amazon EC2 per tuo conto. GuardDuty gestisce anche gli aggiornamenti del security agent.

Per impostazione predefinita, GuardDuty installa il security agent su tutte le istanze del tuo account. Se desideri GuardDuty installare e gestire il security agent solo per istanze EC2 selezionate, aggiungi tag di inclusione o esclusione alle tue istanze EC2, se necessario.

A volte, potresti non voler monitorare gli eventi di runtime per tutte le istanze Amazon EC2 che appartengono al tuo account. Nei casi in cui desideri monitorare gli eventi di runtime per un numero limitato di istanze, aggiungi un tag di inclusione come `GuardDutyManaged: true` a queste istanze selezionate. A partire dalla disponibilità della configurazione automatizzata degli agenti per Amazon EC2, se l'istanza EC2 ha un tag di inclusione (`GuardDutyManaged:true`), GuardDuty rispetterà il tag e gestirà il security agent per le istanze selezionate anche quando non abiliti esplicitamente la configurazione automatica dell'agente.

D'altra parte, se esiste un numero limitato di istanze EC2 per le quali non desideri monitorare gli eventi di runtime, aggiungi un tag di esclusione (`GuardDutyManaged: false`) a queste istanze selezionate. `false` GuardDuty rispetterà il tag di esclusione non installando né gestendo il security agent per queste risorse EC2.

Impatto

Quando utilizzi la configurazione automatizzata degli agenti in un'organizzazione Account AWS o in un'organizzazione, autorizzi GuardDuty a eseguire le seguenti operazioni per tuo conto:

- GuardDuty crea un'associazione SSM per tutte le istanze Amazon EC2 gestite da SSM e visualizzate in Fleet Manager nella console. <https://console.aws.amazon.com/systems-manager/>
- Utilizzo dei tag di inclusione con la configurazione automatica dell'agente disabilitata: dopo aver abilitato il Runtime Monitoring, quando non abiliti la configurazione automatica dell'agente ma aggiungi il tag di inclusione alla tua istanza Amazon EC2, significa che stai autorizzando GuardDuty a gestire il security agent per tuo conto. L'associazione SSM installerà quindi l'agente di sicurezza in ogni istanza che presenta il tag di inclusione (`:GuardDutyManaged: true`)
- Se abiliti la configurazione automatica dell'agente, l'associazione SSM installerà quindi il security agent in tutte le istanze EC2 che appartengono al tuo account.
- Utilizzo dei tag di esclusione con la configurazione automatica degli agenti: prima di abilitare la configurazione automatica degli agenti, quando aggiungi un tag di esclusione alla tua istanza Amazon EC2, significa che stai GuardDuty autorizzando a impedire l'installazione e la gestione del security agent per l'istanza selezionata.

Ora, quando abiliti la configurazione automatizzata dell'agente, l'associazione SSM installerà e gestirà l'agente di sicurezza in tutte le istanze EC2 ad eccezione di quelle contrassegnate con il tag di esclusione.

- GuardDuty crea endpoint VPC in tutti i VPC, compresi i VPC condivisi, purché in quel VPC sia presente almeno un'istanza Linux EC2 che non si trovi nello stato di terminazione o di chiusura dell'istanza. Ciò include il VPC e lo spoke centralizzati. VPCs GuardDuty non supporta la creazione di un endpoint VPC solo per il VPC centralizzato. Per ulteriori informazioni sul funzionamento del VPC centralizzato, consulta [Interface VPC endpoint nel Whitepaper - Creazione di un'infrastruttura di AWS rete multi-VPC](#) scalabile e sicura. AWS

Per informazioni sui diversi stati delle istanze, consulta il [ciclo di vita dell'istanza nella Guida](#) per l'utente di Amazon EC2.

GuardDuty supporta anche. [Utilizzo di un VPC condiviso con Runtime Monitoring](#) Dopo aver considerato tutti i prerequisiti per l'organizzazione Account AWS, GuardDuty utilizzerà il VPC condiviso per ricevere eventi di runtime.

 Note

Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint VPC.

- Oltre all'endpoint VPC, crea GuardDuty anche un nuovo gruppo di sicurezza. Le regole in entrata (ingresso) controllano il traffico autorizzato a raggiungere le risorse associate al gruppo di sicurezza. GuardDuty aggiunge regole in entrata che corrispondono all'intervallo CIDR VPC per la risorsa e si adatta anche quando l'intervallo CIDR cambia. Per ulteriori informazioni, consulta la [gamma VPC CIDR](#) nella Amazon VPC User Guide.

Gestisci l'agente di sicurezza manualmente

Esistono due modi per gestire manualmente l'agente di sicurezza per Amazon EC2:

- Utilizza i documenti GuardDuty gestiti AWS Systems Manager per installare l'agente di sicurezza sulle tue istanze Amazon EC2 che sono già gestite tramite SSM.

Ogni volta che avvii una nuova istanza Amazon EC2, assicurati che sia abilitata SSM.

- Usa gli script RPM Package Manager (RPM) per installare il security agent sulle tue istanze Amazon EC2, indipendentemente dal fatto che siano gestite tramite SSM o meno.

Approfondimenti

Per iniziare a utilizzare la configurazione di Runtime Monitoring per monitorare le istanze Amazon EC2, consulta. [Prerequisiti per il supporto delle istanze Amazon EC2](#)

Come funziona il monitoraggio del runtime con Fargate (solo Amazon ECS)

Quando abiliti il monitoraggio del runtime, GuardDuty diventa pronto a consumare gli eventi di runtime di un'attività. Queste attività vengono eseguite all'interno dei cluster Amazon ECS, che a loro volta vengono eseguiti sulle AWS Fargate istanze. GuardDuty Per ricevere questi eventi di runtime, devi utilizzare il security agent dedicato e completamente gestito.

 Note

Il monitoraggio del runtime non supporta le applicazioni in esecuzione su [Amazon ECS Managed Instances](#).

Puoi consentire la gestione del GuardDuty security agent GuardDuty per tuo conto, utilizzando la configurazione automatizzata dell'agente per un AWS account o un'organizzazione. GuardDuty inizierà a distribuire il security agent nelle nuove attività di Fargate che vengono lanciate nei cluster Amazon ECS. L'elenco seguente specifica cosa aspettarsi quando si abilita il security agent. GuardDuty

Impatto dell'attivazione del GuardDuty Security Agent

GuardDuty crea un endpoint e un gruppo di sicurezza su cloud privato virtuale (VPC)

- Quando si distribuisce il GuardDuty security agent, GuardDuty verrà creato un endpoint VPC attraverso il quale il security agent consegna gli eventi di runtime. GuardDuty

Oltre all'endpoint VPC, crea GuardDuty anche un nuovo gruppo di sicurezza. Le regole in entrata (ingresso) controllano il traffico autorizzato a raggiungere le risorse associate al gruppo di sicurezza. GuardDuty aggiunge regole in entrata che corrispondono all'intervallo CIDR VPC per la risorsa e si adatta anche quando l'intervallo CIDR cambia. Per ulteriori informazioni, consulta la [gamma VPC CIDR](#) nella Amazon VPC User Guide.

- Utilizzo di un VPC centralizzato con agente automatizzato: quando GuardDuty utilizzi la configurazione automatica degli agenti per un tipo di risorsa GuardDuty , creerà un endpoint VPC per tuo conto per tutti. VPCs Ciò include il VPC e lo spoke centralizzati. VPCs GuardDuty non supporta la creazione di un endpoint VPC solo per il VPC centralizzato. Per ulteriori informazioni sul funzionamento del VPC centralizzato, consulta [Interface VPC endpoint nel Whitepaper - Creazione di un'infrastruttura di AWS rete multi-VPC](#) scalabile e sicura. AWS
- Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint VPC.

GuardDuty aggiunge un contenitore sidecar

Per una nuova attività o servizio Fargate che inizia a funzionare, un GuardDuty container (sidecar) si collega a ciascun contenitore all'interno dell'attività Amazon ECS Fargate. L'agente di GuardDuty sicurezza viene eseguito all'interno del contenitore collegato. GuardDuty Questo aiuta GuardDuty a raccogliere gli eventi di runtime di ogni contenitore in esecuzione nell'ambito di queste attività.

L'immagine del contenitore GuardDuty sidecar è archiviata in Amazon Elastic Container Registry (Amazon ECR), con i relativi livelli di immagine archiviati in Amazon S3. Quando l'attività inizia, deve estrarre questa immagine da ECR. A seconda della configurazione di rete, potrebbero essere necessarie impostazioni specifiche per garantire l'accesso sia a ECR che a S3. Ad esempio, se utilizzi gruppi di sicurezza con accesso limitato, dovrai consentire l'accesso all'elenco

dei prefissi gestiti di S3. Per ulteriori informazioni su come effettuare tale operazione, consulta [Prerequisiti per l'accesso all'immagine del contenitore](#).

Quando si avvia un'attività Fargate, se il GuardDuty contenitore (sidecar) non è in grado di avviarsi in uno stato integro, il Runtime Monitoring è progettato per non impedire l'esecuzione delle attività.

Per impostazione predefinita, un'attività Fargate è immutabile. GuardDuty non distribuirà il sidecar quando un'attività è già in esecuzione. Se desideri monitorare un contenitore in un'attività già in esecuzione, puoi interrompere l'attività e riavviarla.

Approcci per gestire gli agenti GuardDuty di sicurezza nelle risorse di Amazon ECS-Fargate

Runtime Monitoring ti offre la possibilità di rilevare potenziali minacce alla sicurezza su tutti i cluster Amazon ECS (a livello di account) o sui cluster selettivi (a livello di cluster) del tuo account. Quando abiliti la configurazione automatizzata degli agenti per ogni attività di Amazon ECS Fargate che verrà eseguita GuardDuty, aggiungerà un contenitore secondario per ogni carico di lavoro del container all'interno di tale attività. L'agente GuardDuty di sicurezza viene distribuito in questo contenitore secondario. In questo modo si GuardDuty ottiene visibilità sul comportamento di runtime dei contenitori all'interno delle attività di Amazon ECS.

Runtime Monitoring supporta la gestione dell'agente di sicurezza per i cluster Amazon ECS (AWS Fargate) solo tramite GuardDuty. Non è disponibile alcun supporto per la gestione manuale del security agent sui cluster Amazon ECS.

Prima di configurare i tuoi account, valuta se desideri monitorare il comportamento di runtime di tutti i contenitori che appartengono alle attività di Amazon ECS o includere o escludere risorse specifiche. Prendi in considerazione i seguenti approcci.

Monitoraggio per tutti i cluster Amazon ECS

Questo approccio ti aiuterà a rilevare potenziali minacce alla sicurezza a livello di account. Utilizza questo approccio quando desideri rilevare potenziali minacce GuardDuty alla sicurezza per tutti i cluster Amazon ECS che appartengono al tuo account.

Escludi cluster Amazon ECS specifici

Utilizza questo approccio quando desideri rilevare potenziali minacce GuardDuty alla sicurezza per la maggior parte dei cluster Amazon ECS nel tuo AWS ambiente ma escluderne alcuni.

Questo approccio ti aiuta a monitorare il comportamento di runtime dei container all'interno delle tue attività Amazon ECS a livello di cluster. Ad esempio, il numero di cluster Amazon ECS che appartengono al tuo account è 1000. Tuttavia, desideri monitorare solo 930 cluster Amazon ECS.

Questo approccio richiede l'aggiunta di un GuardDuty tag predefinito ai cluster Amazon ECS che non desideri monitorare. Per ulteriori informazioni, consulta [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#).

Includi cluster Amazon ECS specifici

Utilizza questo approccio quando desideri GuardDuty rilevare potenziali minacce alla sicurezza per alcuni cluster Amazon ECS. Questo approccio ti aiuta a monitorare il comportamento di runtime dei container all'interno delle tue attività Amazon ECS a livello di cluster. Ad esempio, il numero di cluster Amazon ECS che appartengono al tuo account è 1000. Tuttavia, desideri monitorare solo 230 cluster.

Questo approccio richiede l'aggiunta di un GuardDuty tag predefinito ai cluster Amazon ECS che desideri monitorare. Per ulteriori informazioni, consulta [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#).

Dopo aver abilitato il monitoraggio del runtime

Dopo aver abilitato il Runtime Monitoring e installato il GuardDuty Security Agent nel tuo account standalone o negli account con più membri, puoi eseguire le seguenti operazioni per assicurarti che l'impostazione del piano di protezione funzioni come previsto e monitorare la quantità di memoria e CPU utilizzata dal GuardDuty Security Agent.

Valuta la copertura del runtime

GuardDuty consiglia di valutare continuamente lo stato di copertura della risorsa in cui è stato distribuito il security agent. Lo stato della copertura potrebbe essere Inintegro o Insalubre. Uno stato di copertura integro indica che GuardDuty sta ricevendo gli eventi di runtime dalla risorsa corrispondente quando è in corso un'attività a livello di sistema operativo.

Quando lo stato di copertura diventa Inattivo per la risorsa, GuardDuty è in grado di ricevere gli eventi di runtime e analizzarli per il rilevamento delle minacce. Quando GuardDuty rileva una potenziale minaccia alla sicurezza nelle attività o nelle applicazioni in esecuzione nei carichi di lavoro e nelle istanze del container, genera. GuardDuty [GuardDuty Tipi di risultati del monitoraggio del runtime](#)

Puoi anche configurare un Amazon EventBridge (EventBridge) per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy e altro. Per ulteriori informazioni, consulta [Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi](#).

Configura il monitoraggio della CPU e della memoria per il GuardDuty security agent

Dopo aver verificato che lo stato di copertura risulti integro, puoi valutare le prestazioni del security agent per il tuo tipo di risorsa. Per i cluster Amazon EKS con la release Security Agent v1.5 o successiva, GuardDuty supporta la configurazione dei parametri del security agent (aggiuntivo). Per ulteriori informazioni, consulta [Configurazione del monitoraggio della CPU e della memoria](#).

GuardDuty rileva potenziali minacce

Quando GuardDuty inizia a ricevere gli eventi di runtime della risorsa, inizia ad analizzarli. Quando GuardDuty rileva una potenziale minaccia alla sicurezza in una delle tue istanze Amazon EC2, nei cluster Amazon ECS o nei cluster Amazon EKS, ne genera una o più. [GuardDuty Tipi di risultati del monitoraggio del runtime](#) Puoi accedere ai dettagli dei risultati per visualizzare i dettagli delle risorse interessate.

Come funziona la versione di prova gratuita di 30 giorni in Runtime Monitoring

Il periodo di prova gratuito di 30 giorni funziona in modo diverso per i nuovi GuardDuty account e per gli account esistenti che hanno già abilitato EKS Runtime Monitoring prima che la funzionalità di Runtime Monitoring fosse estesa alle istanze Amazon EC2 e AWS Fargate (solo Amazon ECS).

Sto usando il periodo di GuardDuty prova o non ho mai abilitato EKS Runtime Monitoring

L'elenco seguente spiega come funziona il periodo di prova gratuito di 30 giorni se utilizzi il periodo di prova di GuardDuty 30 giorni o non hai mai abilitato EKS Runtime Monitoring:

- Quando si abilita GuardDuty per la prima volta, il Runtime Monitoring e EKS Runtime Monitoring non saranno abilitati per impostazione predefinita.

Quando abiliti il Runtime Monitoring per il tuo account o la tua organizzazione, assicurati di configurare anche il GuardDuty security agent per la risorsa che desideri monitorare per il rilevamento delle minacce. Ad esempio, se desideri utilizzare Runtime Monitoring per le tue

istanze Amazon EC2, dopo aver abilitato il Runtime Monitoring, devi configurare anche l'agente di sicurezza per Amazon EC2. Puoi scegliere di farlo manualmente o automaticamente tramite GuardDuty

- Il piano di protezione del Runtime Monitoring è abilitato a livello di account. Il periodo di prova gratuito di 30 giorni funziona a livello di risorse. Dopo la distribuzione del GuardDuty Security Agent su un tipo di risorsa specifico, la prova gratuita di 30 giorni inizia quando GuardDuty riceve il primo evento di runtime associato a questo tipo di risorsa. Ad esempio, hai distribuito l' GuardDuty agente a livello di risorsa (per l'istanza Amazon EC2, il cluster Amazon ECS e il cluster Amazon EKS). Quando GuardDuty riceve il primo evento di runtime per un'istanza Amazon EC2, la prova gratuita di 30 giorni inizierà solo per Amazon EC2.
- Quando desideri abilitare solo EKS Runtime Monitoring — Quando lo abiliti GuardDuty per la prima volta, EKS Runtime Monitoring non è abilitato per impostazione predefinita (dopo il rilascio di Runtime Monitoring). Dovrai abilitare EKS Runtime Monitoring. Per utilizzarlo in modo ottimale, assicuratevi di gestire il GuardDuty security agent manualmente o di abilitare la configurazione automatizzata dell'agente in modo che GuardDuty gestisca l'agente per vostro conto. Il periodo di prova gratuito di 30 giorni per EKS Runtime Monitoring inizia quando GuardDuty riceve il primo evento di runtime per la risorsa Amazon EKS.

Ho abilitato EKS Runtime Monitoring prima del lancio di Runtime Monitoring

Utilizza questa sezione solo quando EKS Runtime Monitoring era abilitato per te Account AWS e ora desideri migrare a Runtime Monitoring.

L'elenco seguente include scenari che potrebbero applicarsi al vostro caso d'uso di abilitazione del Runtime Monitoring:

- Per un GuardDuty account esistente che ha il piano di protezione EKS Runtime Monitoring abilitato e utilizza l'esperienza della GuardDuty console per utilizzare questo piano di protezione: con l'annuncio di Runtime Monitoring, l'esperienza della console EKS Runtime Monitoring è stata ora consolidata nel Runtime Monitoring. La configurazione esistente per EKS Runtime Monitoring rimane la stessa. È possibile continuare a utilizzare il supporto API/CLI per eseguire operazioni associate a EKS Runtime Monitoring.
- Per utilizzare EKS Runtime Monitoring come parte del Runtime Monitoring, è necessario configurare il Runtime Monitoring per l'account o l'organizzazione. Per mantenere la stessa configurazione per Runtime Monitoring, vedi [Migrazione da EKS Runtime Monitoring a Runtime Monitoring](#). Tuttavia, ciò non influirà sulla prova gratuita di 30 giorni per la risorsa Amazon EKS.

- Il piano di protezione del Runtime Monitoring è abilitato a livello di account per regione. Dopo la distribuzione del GuardDuty security agent su uno dei tipi di risorse specificati (istanza Amazon EC2 e cluster Amazon ECS), la prova gratuita di 30 giorni inizia GuardDuty quando riceve il primo evento di runtime associato alla risorsa. È disponibile una prova gratuita di 30 giorni associata a ciascun tipo di risorsa.

Ad esempio, dopo aver abilitato il Runtime Monitoring, scegli di distribuire l' GuardDuty agente solo su un'istanza Amazon EC2, la prova gratuita di 30 giorni per questa risorsa inizierà solo GuardDuty quando riceverà il primo evento di runtime per un'istanza Amazon EC2. Successivamente, quando distribuirai l' GuardDuty agente per Fargate (solo Amazon ECS), la prova gratuita di 30 giorni per questa risorsa inizierà solo GuardDuty quando riceverà il primo evento di runtime per il cluster Amazon ECS. Considerando che hai già abilitato EKS Runtime Monitoring per il tuo account, GuardDuty non ripristina la prova gratuita di 30 giorni per una risorsa Amazon EKS.

Prerequisiti per abilitare il monitoraggio del runtime

Per abilitare il Runtime Monitoring e gestire il GuardDuty security agent, è necessario soddisfare i prerequisiti per ogni tipo di risorsa che si desidera monitorare per il rilevamento delle minacce. Ogni tipo di risorsa presenta prerequisiti diversi. Ad esempio, GuardDuty supporta diverse distribuzioni del sistema operativo in base al tipo di risorsa.

Se desideri monitorare solo le risorse Amazon EC2, devi rispettare i prerequisiti per le istanze Amazon EC2. Se in un secondo momento scegli di monitorare le risorse Amazon EKS, devi rispettare i prerequisiti specifici dei cluster Amazon EKS.

Le seguenti sezioni includono i prerequisiti in base al tipo di risorsa.

Indice

- [Prerequisiti per il supporto delle istanze Amazon EC2](#)
- [Prerequisiti per il AWS Fargate supporto \(solo Amazon ECS\)](#)
- [Prerequisiti per il supporto dei cluster Amazon EKS](#)

Prerequisiti per il supporto delle istanze Amazon EC2

Questa sezione include i prerequisiti per il monitoraggio del comportamento di runtime delle istanze Amazon EC2. Una volta soddisfatti questi prerequisiti, consulta. [Abilitazione del monitoraggio del GuardDuty runtime](#)

Argomenti

- [Rendi le istanze EC2 gestite tramite SSM \(solo per la configurazione automatica degli agenti\)](#)
- [Convalida i requisiti architetturici](#)
- [Convalida della politica di controllo dei servizi della tua organizzazione in un ambiente con più account](#)
- [Quando si utilizza la configurazione automatica degli agenti](#)
- [Limite di CPU e memoria per l'agente GuardDuty](#)
- [Approfondimenti](#)

Rendi le istanze EC2 gestite tramite SSM (solo per la configurazione automatica degli agenti)

GuardDuty utilizza AWS Systems Manager (SSM) per distribuire, installare e gestire automaticamente il security agent sulle tue istanze. Se si prevede di installare e gestire manualmente l' GuardDuty agente, l'SSM non è necessario.

Per gestire le istanze Amazon EC2 con Systems Manager, consulta [Configurazione delle istanze di Systems Manager per Amazon EC2 nella Guida per l'utente](#).AWS Systems Manager

Convalida i requisiti architetturici

L'architettura della distribuzione del sistema operativo potrebbe influire sul comportamento del GuardDuty Security Agent. È necessario soddisfare i seguenti requisiti prima di utilizzare Runtime Monitoring per le istanze Amazon EC2:

- Il supporto del kernel include eBPF e. Tracepoints Kprobe Per le architetture CPU, Runtime Monitoring supporta AMD64 (x64) e ARM64 (Graviton2 e versioni successive). ¹

La tabella seguente mostra la distribuzione del sistema operativo che è stata verificata per supportare l'agente GuardDuty di sicurezza per le istanze Amazon EC2.

distribuzione del sistema operativo ²	Versione del kernel ³
Amazon Linux 2	5.4 ⁴ , 5.10, 5.15 ⁴

distribuzione del sistema operativo ²	Versione del kernel ³
Amazon Linux 2023	5.4 ⁴ , 5.10, 5.15, ⁴ 6.1, 6.5, 6.8, 6,12
Ubuntu 20.04 e Ubuntu 22.04	5.4 ⁴ , 5.10, 5.15, ⁴ 6.1, 6.5, 6.8
Debian 11 e Debian 12	5.4 ⁴ , 5.10, 5.15, ⁴ 6.1, 6.5, 6.8
Ubuntu 24.04	6.8 6,13, 6,14 ⁵
RedHat 9.4	5,14
Fedora 34.0	5.11, 5.17
Fedora 40	6.8
Fedora 41	6.12
CentOS Stream 9	5,14
Oracle Linux 8.9	5.15
Oracle Linux 9.3	5.15
Rocky Linux 9.5	5.14
Alma Linux 9	5.14
Alma Linux 10	6.12
SUSE Linux Enterprise Server 16	6.12

1. Il monitoraggio del runtime per le risorse Amazon EC2 non supporta le istanze Graviton di prima generazione come i tipi di istanze A1.

2. Supporto per vari sistemi operativi: GuardDuty ha verificato il supporto del Runtime Monitoring per la distribuzione operativa elencata nella tabella precedente. Sebbene il GuardDuty security agent possa funzionare su sistemi operativi non elencati nella tabella precedente, il GuardDuty team non può garantire il valore di sicurezza previsto.
 3. Per qualsiasi versione del kernel, è necessario impostare il `CONFIG_DEBUG_INFO_BTF` flag su `y` (che significa true). Ciò è necessario per consentire al GuardDuty Security Agent di funzionare come previsto.
 4. Per le versioni del kernel 5.10 e precedenti, il GuardDuty security agent utilizza la memoria bloccata nella RAM (`RLIMIT_MEMLOCK`) per funzionare come previsto. Se il `RLIMIT_MEMLOCK` valore del sistema è impostato su un valore troppo basso, si GuardDuty consiglia di impostare i limiti rigidi e morbidi su almeno 32 MB. Per informazioni sulla verifica e la modifica del `RLIMIT_MEMLOCK` valore predefinito, vedere. [Visualizzazione e aggiornamento dei valori `RLIMIT\_MEMLOCK`](#)
 5. Per Ubuntu 24.04, le versioni del kernel 6.13 e 6.14 supportano solo le versioni dell'agente EC2 1.9.2 e successive.
- Requisiti aggiuntivi: solo se disponi di Amazon ECS/Amazon EC2

Per Amazon ECS/Amazon EC2, ti consigliamo di utilizzare la versione più recente ottimizzata per Amazon ECS AMIs (datata 29 settembre 2023 o successiva) o di utilizzare la versione dell'agente Amazon ECS v1.77.0.

Visualizzazione e aggiornamento dei valori **RLIMIT_MEMLOCK**

Quando il `RLIMIT_MEMLOCK` limite del sistema è troppo basso, il GuardDuty Security Agent potrebbe non funzionare come previsto. GuardDuty raccomanda che sia i limiti rigidi che quelli flessibili siano di almeno 32 MB. Se non aggiorni i limiti, non GuardDuty sarà possibile monitorare gli eventi di runtime della risorsa. Quando `RLIMIT_MEMLOCK` supera i limiti minimi indicati, l'aggiornamento di tali limiti diventa facoltativo.

È possibile modificare il `RLIMIT_MEMLOCK` valore predefinito prima o dopo l'installazione del GuardDuty Security Agent.

Per visualizzare **RLIMIT_MEMLOCK** i valori

1. Esegui `ps aux | grep guardduty`. Questo produrrà l'ID del processo (pid).
2. Copia l'ID del processo (pid) dall'output del comando precedente.
3. Esegui `grep "Max locked memory" /proc/pid/limits` dopo averlo sostituito pid con l'ID di processo copiato dal passaggio precedente.

Verrà visualizzata la quantità massima di memoria bloccata per l'esecuzione del GuardDuty Security Agent.

Per aggiornare **RLIMIT_MEMLOCK** i valori

1. Se il `/etc/systemd/system.conf.d/NUMBER-limits.conf` file esiste, commenta la riga `DefaultLimitMEMLOCK` di questo file. Questo file imposta un valore predefinito `RLIMIT_MEMLOCK` con priorità alta, che sovrascrive le impostazioni nel `/etc/systemd/system.conf` file.
2. Apri il `/etc/systemd/system.conf` file e decommenta la riga che contiene `#DefaultLimitMEMLOCK=`
3. Aggiorna il valore predefinito fornendo `RLIMIT_MEMLOCK` limiti rigidi e flessibili di almeno 32 MB. L'aggiornamento dovrebbe assomigliare a questo: `DefaultLimitMEMLOCK=32M:32M`. Il formato è `soft-limit:hard-limit`.
4. Esegui `sudo reboot`.

Convalida della politica di controllo dei servizi della tua organizzazione in un ambiente con più account

Se hai impostato una policy di controllo dei servizi (SCP) per gestire le autorizzazioni nella tua organizzazione, verifica che il limite delle autorizzazioni consenta l'azione `guardduty:SendSecurityTelemetry`. È necessario per supportare il monitoraggio del runtime GuardDuty su diversi tipi di risorse.

Se sei un account membro, connettiti con l'amministratore delegato associato. Per informazioni sulla gestione SCPs dell'organizzazione, consulta [le politiche di controllo del servizio \(SCPs\)](#).

Quando si utilizza la configurazione automatica degli agenti

Per [Utilizza la configurazione automatica degli agenti \(scelta consigliata\)](#) farlo, Account AWS è necessario soddisfare i seguenti prerequisiti:

- Quando utilizzi tag di inclusione con configurazione automatica degli agenti, per GuardDuty creare un'associazione SSM per una nuova istanza, assicurati che la nuova istanza sia gestita tramite SSM e venga visualizzata in Fleet Manager nella console. <https://console.aws.amazon.com/systems-manager/>
- Quando si utilizzano i tag di esclusione con la configurazione automatica degli agenti:
 - Aggiungi il `false` tagGuardDutyManaged: prima di configurare l'agente GuardDuty automatico per il tuo account.

Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle.

Dopo aver abilitato la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

- Abilita l'opzione Consenti tag nelle impostazioni dei metadati per le tue istanze. Questa impostazione è necessaria perché GuardDuty deve leggere il tag di esclusione dall'Instance Metadata Service (IMDS) per determinare se escludere l'istanza dall'installazione dell'agente. Per ulteriori informazioni, consulta [Abilita l'accesso ai tag nei metadati dell'istanza nella Guida](#) per l'utente di Amazon EC2.

Limite di CPU e memoria per l'agente GuardDuty

Limite della CPU

Il limite massimo di CPU per il GuardDuty security agent associato alle istanze Amazon EC2 è pari al 10% dei core vCPU totali. Ad esempio, se l'istanza EC2 ha 4 core vCPU, il security agent può utilizzare al massimo il 40 per cento del 400 per cento totale disponibile.

Memory limit (Limite memoria)

Dalla memoria associata all'istanza Amazon EC2, c'è una memoria limitata che il GuardDuty security agent può utilizzare.

La tabella seguente mostra il limite di memoria.

Memoria dell'istanza Amazon EC2	Memoria massima per l'agente GuardDuty
Meno di 8 GB	128 MB
Meno di 32 GB	256 MB
Maggiore o uguale a 32 GB	1 GB

Approfondimenti

Il passaggio successivo consiste nella configurazione del Runtime Monitoring e nella gestione del security agent (automaticamente o manualmente).

Prerequisiti per il AWS Fargate supporto (solo Amazon ECS)

Questa sezione include i prerequisiti per il monitoraggio del comportamento di runtime delle risorse Fargate-Amazon ECS. Una volta soddisfatti questi prerequisiti, vedere. [Abilitazione del monitoraggio del GuardDuty runtime](#)

Argomenti

- [Convalida dei requisiti relativi all'architettura](#)
- [Prerequisiti per l'accesso all'immagine del contenitore](#)
- [Convalida della politica di controllo dei servizi dell'organizzazione in un ambiente con più account](#)
- [Convalida delle autorizzazioni dei ruoli e del limite delle autorizzazioni delle policy](#)
- [Limiti di CPU e di memoria](#)

Convalida dei requisiti relativi all'architettura

La piattaforma utilizzata può influire sul modo GuardDuty in cui il GuardDuty Security Agent supporta la ricezione degli eventi di runtime dai cluster Amazon ECS. Devi confermare di utilizzare una delle piattaforme verificate.

Considerazioni iniziali:

La AWS Fargate piattaforma per i tuoi cluster Amazon ECS deve essere Linux. La versione della piattaforma corrispondente deve essere almeno 1.4.0, o. LATEST Per ulteriori informazioni

sulle versioni della piattaforma, consulta le versioni della [piattaforma Linux](#) nella Amazon Elastic Container Service Developer Guide.

Le versioni della piattaforma Windows non sono ancora supportate.

Piattaforme verificate

La distribuzione del sistema operativo e l'architettura della CPU influiscono sul supporto fornito dal GuardDuty security agent. La tabella seguente mostra la configurazione verificata per la distribuzione del GuardDuty security agent e la configurazione del Runtime Monitoring.

distribuzione del sistema operativo ¹	Supporto del kernel	Architettura CPU x64 () AMD64	Architettura CPU Graviton () ARM64
Linux	eBPF, Tracepoints, Kprobe	Supportata	Supportata

¹ Supporto per vari sistemi operativi: GuardDuty ha verificato il supporto del Runtime Monitoring per la distribuzione operativa elencata nella tabella precedente. Sebbene il GuardDuty security agent possa funzionare su sistemi operativi non elencati nella tabella precedente, il GuardDuty team non può garantire il valore di sicurezza previsto.

Prerequisiti per l'accesso all'immagine del contenitore

I seguenti prerequisiti consentono di accedere all'immagine del contenitore GuardDuty sidecar dal repository Amazon ECR.

Requisiti per le autorizzazioni

Il ruolo di esecuzione dell'attività richiede determinate autorizzazioni Amazon Elastic Container Registry (Amazon ECR) per scaricare l'immagine del contenitore GuardDuty del Security Agent:

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

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

Per limitare ulteriormente le autorizzazioni di Amazon ECR, puoi aggiungere l'URI del repository Amazon ECR che ospita l'agente di GuardDuty sicurezza per (solo AWS Fargate Amazon ECS). Per ulteriori informazioni, consulta [Agente di hosting del repository Amazon ECR GuardDuty](#).

Puoi utilizzare la policy ECSTask ExecutionRolePolicy gestita da [Amazon](#) o aggiungere le autorizzazioni di cui sopra alla tua TaskExecutionRole politica.

Configurazione della definizione dell'attività

Quando crei o aggiorni i servizi Amazon ECS, devi fornire informazioni sulla sottorete nella definizione dell'attività:

L'esecuzione di [CreateService](#) e [UpdateService](#) APIs nell'Amazon Elastic Container Service API Reference richiede il trasferimento delle informazioni sulla sottorete. Per ulteriori informazioni, consulta le [definizioni delle attività di Amazon ECS](#) nella Amazon Elastic Container Service Developer Guide.

Requisiti di connessione di rete

È necessario garantire la connettività di rete per scaricare l'immagine del GuardDuty contenitore da Amazon ECR. Questo requisito è specifico GuardDuty perché utilizza Amazon ECR per ospitare il suo agente di sicurezza. A seconda della configurazione di rete, è necessario implementare una delle seguenti opzioni:

Opzione 1: utilizzo dell'accesso alla rete pubblica (se disponibile)

Se le attività di Fargate vengono eseguite in sottoreti con accesso a Internet in uscita, non è richiesta alcuna configurazione di rete aggiuntiva.

Opzione 2: utilizzo degli endpoint Amazon VPC (per sottoreti private)

Se le attività Fargate vengono eseguite in sottoreti private senza accesso a Internet, è necessario configurare gli endpoint VPC per ECR per garantire che l'URI del repository ECR che ospita il security agent sia accessibile dalla rete. GuardDuty Senza questi endpoint, le attività nelle sottoreti private non possono scaricare l'immagine del contenitore. GuardDuty

Per le istruzioni sulla configurazione degli endpoint VPC, consulta Create [the VPC endpoint for Amazon ECR nella Amazon](#) Elastic Container Registry User Guide.

Per informazioni su come abilitare Fargate a scaricare il GuardDuty contenitore, consulta [Using Amazon ECR images with Amazon ECS nella Amazon Elastic Container Registry User Guide](#).

Configurazione del gruppo di sicurezza

Le immagini dei GuardDuty container sono in Amazon ECR e richiedono l'accesso ad Amazon S3. Questo requisito è specifico per il download di immagini di container da Amazon ECR. Per le attività con accesso limitato alla rete, è necessario configurare i gruppi di sicurezza per consentire l'accesso a S3.

Aggiungi una regola in uscita nel tuo gruppo di sicurezza che consenta il traffico verso [l'elenco dei prefissi gestiti di S3 \(p1-xxxxxxx\)](#) sulla porta 443. Per aggiungere una regola in uscita, consulta [Configura le regole dei gruppi di sicurezza](#) nella Amazon VPC User Guide.

Per visualizzare gli elenchi di prefissi AWS-managed nella console o descriverli utilizzando AWS Command Line Interface (AWS CLI), consulta [AWS-managed prefix lists nella Amazon VPC User Guide](#).

Convalida della politica di controllo dei servizi dell'organizzazione in un ambiente con più account

Questa sezione spiega come convalidare le impostazioni della policy di controllo del servizio (SCP) per garantire che il Runtime Monitoring funzioni come previsto in tutta l'organizzazione.

Se avete impostato una o più politiche di controllo del servizio per gestire le autorizzazioni nella vostra organizzazione, dovete verificare che l'azione non venga negata.

`guardduty:SendSecurityTelemetry` Per informazioni su come SCPs funziona, consulta la [valutazione SCP](#) nella Guida per l'utente.AWS Organizations

Se sei un account membro, connettiti con l'amministratore delegato associato. Per informazioni sulla gestione SCPs dell'organizzazione, consulta [le politiche di controllo del servizio \(SCPs\)](#) nella Guida per l'AWS Organizations utente.

Esegui i passaggi seguenti per tutto SCPs ciò che hai configurato nel tuo ambiente multi-account:

La convalida non **`guardduty:SendSecurityTelemetry`** è negata in SCP

1. Accedi alla console Organizations all'indirizzo <https://console.aws.amazon.com/organizations/>. Devi accedere come ruolo IAM o accedere come utente root ([scelta non consigliata](#)) nell'account di gestione dell'organizzazione.

2. Nel riquadro di navigazione a sinistra, seleziona Policies (Policy). Quindi, in Tipi di policy supportati, seleziona Service control policies.
3. Nella pagina Criteri di controllo del servizio, scegli il nome della politica che desideri convalidare.
4. Nella pagina dei dettagli della politica, visualizza il contenuto di questa politica. Assicurati che non neghi `guardduty:SendSecurityTelemetry`.

La seguente politica SCP è un esempio di come non negare l'azione:
`guardduty:SendSecurityTelemetry`

JSON

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

Se la tua politica nega questa azione, devi aggiornare la politica. Per ulteriori informazioni, consulta [Aggiornamento di una policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .

Convalida delle autorizzazioni dei ruoli e del limite delle autorizzazioni delle policy

Utilizza i seguenti passaggi per verificare che i limiti delle autorizzazioni associati al ruolo e alla relativa politica non influiscano sull'azione di restrizione. `guardduty:SendSecurityTelemetry`

Per visualizzare i limiti delle autorizzazioni per i ruoli e la relativa politica

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli.

3. Nella pagina Ruoli, seleziona il ruolo *TaskExecutionRole* che potresti aver creato.
4. Nella pagina del ruolo selezionato, nella scheda Autorizzazioni, espandi il nome della policy associata a questo ruolo. Quindi, verifica che questa politica non preveda restrizioni. `guardduty:SendSecurityTelemetry`
5. Se il limite delle autorizzazioni è impostato, espandi questa sezione. Quindi, espandi ogni politica per verificare che non limiti l'azione `guardduty:SendSecurityTelemetry`. La politica dovrebbe apparire simile a questa [Example SCP policy](#).

Se necessario, esegui una delle seguenti azioni:

- Per modificare la politica, seleziona Modifica. Nella pagina Modifica le autorizzazioni per questa politica, aggiorna la politica nell'editor delle politiche. Assicurati che lo schema JSON rimanga valido. Quindi, seleziona Successivo. Quindi, puoi rivedere e salvare le modifiche.
- Per modificare questo limite di autorizzazioni e scegliere un altro limite, scegli Cambia limite.
- Per rimuovere questo limite di autorizzazioni, scegli Rimuovi limite.

Per informazioni sulla gestione delle policy, consulta Policies [and permissions AWS Identity and Access Management nella](#) IAM User Guide.

Limiti di CPU e di memoria

Nella definizione dell'attività Fargate, è necessario specificare il valore della CPU e della memoria a livello di attività. La tabella seguente mostra le combinazioni valide di valori di CPU e memoria a livello di task e il limite massimo di memoria del GuardDuty Security Agent corrispondente per il contenitore. GuardDuty

Valore CPU	Valore memoria	GuardDuty limite massimo di memoria dell'agente
256 (0,25 vCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	

Valore CPU	Valore memoria	GuardDuty limite massimo di memoria dell'agente
2048 (2 vCPU)	Tra 4 GB e 16 GB in incrementi di 1 GB	
4096 (4 vCPU)	Tra 8 GB e 20 GB con incrementi di 1 GB	
8192 (8 vCPU)	Tra 16 GB e 28 GB con incrementi di 4 GB	256 MB
	Tra 32 GB e 60 GB con incrementi di 4 GB	512 MB
16384 (16 vCPU)	Tra 32 GB e 120 GB in incrementi di 8 GB	1 GB

Dopo aver abilitato il Runtime Monitoring e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di Container Insight. Per ulteriori informazioni, consulta [Configurazione del monitoraggio sul cluster Amazon ECS](#).

Il passaggio successivo consiste nel configurare Runtime Monitoring e configurare anche il security agent.

Prerequisiti per il supporto dei cluster Amazon EKS

Questa sezione include i prerequisiti per il monitoraggio del comportamento di runtime delle risorse Amazon EKS. Questi prerequisiti sono fondamentali affinché l' GuardDuty agente funzioni come previsto. Una volta soddisfatti questi prerequisiti, consultate [Abilitazione del monitoraggio del GuardDuty runtime](#) per iniziare a monitorare le vostre risorse.

Support per le funzionalità di Amazon EKS

Runtime Monitoring supporta i cluster Amazon EKS in esecuzione su istanze Amazon EC2 e Amazon EKS Auto Mode.

Runtime Monitoring non supporta i cluster Amazon EKS con Amazon EKS Hybrid Nodes e quelli in AWS Fargate esecuzione.

Per informazioni su queste funzionalità di Amazon EKS, consulta [Cos'è Amazon EKS?](#) nella Guida per l'utente di Amazon EKS.

Convalida dei requisiti relativi all'architettura

La piattaforma utilizzata può influire sul modo GuardDuty in cui GuardDuty Security Agent supporta la ricezione degli eventi di runtime dai cluster EKS. Devi confermare di utilizzare una delle piattaforme verificate. Se gestisci l' GuardDuty agente manualmente, assicurati che la versione di Kubernetes supporti la versione dell' GuardDuty agente attualmente in uso.

Piattaforme verificate

La distribuzione del sistema operativo, la versione del kernel e l'architettura della CPU influiscono sul supporto fornito dal security agent. GuardDuty Il supporto del kernel include eBPF eTracepoints. Kprobe Per le architetture CPU, Runtime Monitoring supporta AMD64 (x64) e ARM64 (Graviton2 e versioni successive). ¹

La tabella seguente mostra la configurazione verificata per l'implementazione del GuardDuty security agent e la configurazione di EKS Runtime Monitoring.

distribuzione del sistema operativo ²	Versione del kernel ³	Versione di Kubernetes supportata
Portabottiglie	5.4, 5.10, 5.15, 6.1 ⁴	v1.23 - v1.35
Ubuntu	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.35
Amazon Linux 2	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.35
Amazon Linux 2023 ⁵	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.35
RedHat 9.4	5,14 ⁴	v1.21 - v1.35
Fedora 34	5.11, 5,17	v1.21 - v1.35
Fedora 40	6.8	v1.28 - v1.35
Fedora 41	6.12	v1.28 - v1.35

distribuzione del sistema operativo ²	Versione del kernel ³	Versione di Kubernetes supportata
CentOS Stream 9	5.14	v1.21 - v1.35

1. Il monitoraggio del runtime per i cluster Amazon EKS non supporta le istanze Graviton di prima generazione come i tipi di istanze A1.
2. Supporto per vari sistemi operativi: GuardDuty ha verificato il supporto del Runtime Monitoring per la distribuzione operativa elencata nella tabella precedente. Sebbene il GuardDuty security agent possa funzionare su sistemi operativi non elencati nella tabella precedente, il GuardDuty team non può garantire il valore di sicurezza previsto.
3. Per qualsiasi versione del kernel, è necessario impostare il CONFIG_DEBUG_INFO_BTTF flag su y (che significa true). Ciò è necessario per consentire al GuardDuty Security Agent di funzionare come previsto.
4. Attualmente, con la versione Kernel6.1, non è GuardDuty possibile generare dati [GuardDuty Tipi di risultati del monitoraggio del runtime](#) correlati a. [Eventi del Domain Name System \(DNS\)](#)
5. Il monitoraggio del runtime è supportato AL2023 con il rilascio del GuardDuty security agent v1.6.0 e versioni successive. Per ulteriori informazioni, consulta [GuardDuty versioni degli agenti di sicurezza per le risorse Amazon EKS](#).

Versioni di Kubernetes supportate dal security agent GuardDuty

La tabella seguente mostra le versioni di Kubernetes per i cluster EKS supportate dal Security Agent GuardDuty

Versione dell'agente di GuardDuty sicurezza aggiuntivo Amazon EKS	Versione di Kubernetes
v1.12.1 (più recente - v1.12.1-eksbuild.2)	1,28 - 1,35
v1.11.0 (più recente - v1.11.0-eksbuild.4)	1,28 - 1,34

Versione dell'agente di GuardDuty sicurezza aggiuntivo Amazon EKS	Versione di Kubernetes
v1.10.0 (più recente - v1.10.0-eksbuild.2)	1.21 - 1.33
v1.9.0 (più recente - v1.9.0-eksbuild.2)	1,21 - 1,32
v1.8.1 (più recente - v1.8.1-eksbuild.2)	
versione 1.7.1	
v1.7.0	1,21 - 1,31
v1.6.1	
v1.6.0	
v1.5.0	1,21 - 1,29
v1.4.1	
v1.4.0	
v1.3.1	
v1.3.0	
v1.2.0	1,21 - 1,28
v1.1.0	
v1.0.0	1,21 - 1,25

Alcune versioni del GuardDuty Security Agent raggiungeranno la fine del supporto standard.

Per informazioni sulle versioni di rilascio dell'agente, vedere. [GuardDuty versioni degli agenti di sicurezza per le risorse Amazon EKS](#)

Limiti di CPU e di memoria

La tabella seguente mostra i limiti di CPU e memoria per il componente aggiuntivo Amazon EKS per GuardDuty (aws-guardduty-agent).

Parametro	Limite minimo	Limite massimo
CPU	200 m	1000 m
Memoria	256 Mi	1024 Mi

Quando utilizzi il componente aggiuntivo Amazon EKS versione 1.5.0 o successiva, GuardDuty offre la possibilità di configurare lo schema del componente aggiuntivo per i valori di CPU e memoria. Per informazioni sull'intervallo configurabile, consulta [Parametri e valori configurabili](#)

Dopo aver abilitato il monitoraggio del runtime EKS e valutato lo stato di copertura dei cluster EKS, puoi configurare e visualizzare i parametri di Container Insights. Per ulteriori informazioni, consulta [Configurazione del monitoraggio della CPU e della memoria](#).

Convalida della politica di controllo dei servizi dell'organizzazione

Se hai impostato una policy di controllo dei servizi (SCP) per gestire le autorizzazioni nella tua organizzazione, verifica che il limite delle autorizzazioni non sia restrittivo. `guardduty:SendSecurityTelemetry` È necessario per supportare il monitoraggio del runtime GuardDuty su diversi tipi di risorse.

Se sei un account membro, connettiti con l'amministratore delegato associato. Per informazioni sulla gestione SCPs dell'organizzazione, consulta [le politiche di controllo del servizio \(SCPs\)](#).

Abilitazione del monitoraggio del GuardDuty runtime

Prima di abilitare il monitoraggio del runtime nel tuo account, assicurati che il tipo di risorsa per cui desideri monitorare gli eventi di runtime supporti i requisiti della piattaforma. Per ulteriori informazioni, consulta [Prerequisiti](#).

Se avete utilizzato EKS Runtime Monitoring prima del lancio di Runtime Monitoring, potete utilizzare il APIs per controllare e aggiornare la configurazione esistente per EKS Runtime Monitoring. È inoltre possibile migrare la configurazione esistente da EKS Runtime Monitoring a Runtime Monitoring. Per ulteriori informazioni, consulta [Migrazione da EKS Runtime Monitoring a Runtime Monitoring](#).

 Note

Attualmente, questa documentazione fornisce i passaggi per abilitare il monitoraggio del runtime per gli account e l'organizzazione solo tramite console. Puoi anche abilitare il monitoraggio del runtime utilizzando [API Actions](#) o [AWS CLI for GuardDuty](#).

È possibile configurare Runtime Monitoring utilizzando i passaggi descritti nei seguenti argomenti.

Indice

- [Abilitazione del monitoraggio del runtime per ambienti con più account](#)
- [Abilitare il monitoraggio del runtime per un account autonomo](#)

Abilitazione del monitoraggio del runtime per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare il monitoraggio del runtime per gli account membro e gestire la configurazione automatica degli agenti per i tipi di risorse appartenenti agli account membro dell'organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta [Gestione di più account](#).

Per l'account amministratore delegato GuardDuty

Per abilitare il monitoraggio del runtime per l'account amministratore delegato GuardDuty

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Utilizzando Abilita per tutti gli account

Se desideri abilitare il monitoraggio del runtime per tutti gli account che appartengono all'organizzazione, incluso l'account GuardDuty amministratore delegato, scegli Abilita per tutti gli account.

5. Utilizzando Configura gli account manualmente

Se desideri abilitare il monitoraggio del runtime per ogni account membro singolarmente, scegli Configura gli account manualmente.

- Scegli Abilita nella sezione Amministratore delegato (questo account).

6. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)
- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)

Per tutti gli account dei membri

Per abilitare il monitoraggio del runtime per tutti gli account membri dell'organizzazione

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando l'account GuardDuty amministratore delegato.

2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella pagina Runtime Monitoring, nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Scegli Abilita per tutti gli account.
5. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)

- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)

Per tutti gli account membri attivi esistenti

Per abilitare il monitoraggio del runtime per gli account dei membri esistenti nell'organizzazione

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando l'account GuardDuty amministratore delegato dell'organizzazione.

2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella pagina Runtime Monitoring, nella scheda Configurazione, puoi visualizzare lo stato corrente della configurazione di Runtime Monitoring.
4. Nel riquadro Runtime Monitoring, nella sezione Account dei membri attivi, scegli Azioni.
5. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
6. Scegli Conferma.
7. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)
- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)

 Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Abilita automaticamente il monitoraggio del runtime solo per gli account dei nuovi membri

Per abilitare il monitoraggio del runtime per gli account dei nuovi membri dell'organizzazione

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando l'account GuardDuty amministratore delegato designato dell'organizzazione.

2. Nel riquadro di navigazione, scegli Runtime Monitoring
3. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Scegli Configura gli account manualmente.
5. Seleziona Abilita automaticamente per i nuovi account membri.
6. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)
- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)

Solo per account di membri attivi selettivi

Per abilitare il monitoraggio del runtime per i singoli account dei membri attivi

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, rivedi automaticamente i valori nelle colonne Runtime Monitoring e Manage agent. Questi valori indicano se il monitoraggio del runtime e la gestione degli GuardDuty agenti sono abilitati o meno per l'account corrispondente.

4. Dalla tabella Account, selezionate l'account per il quale desiderate abilitare il Runtime Monitoring. Puoi scegliere più account alla volta.
5. Scegli Conferma.
6. Scegli Modifica piani di protezione. Scegliere l'operazione appropriata.
7. Scegli Conferma.
8. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)
- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)

Abilitare il monitoraggio del runtime per un account autonomo

A un account autonomo spetta la decisione di abilitare o disabilitare un piano di protezione Account AWS in uno specifico account. Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione del monitoraggio del runtime per ambienti con più account](#).

Dopo aver abilitato il Runtime Monitoring, assicurati GuardDuty di installare Security Agent tramite la configurazione automatica o la distribuzione manuale. Come parte del completamento di tutti i passaggi elencati nella procedura seguente, assicuratevi di installare il security agent.

Per abilitare il monitoraggio del runtime in un account autonomo

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Abilita per abilitare il monitoraggio del runtime per il tuo account.

4. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)
- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)

Gestione degli agenti GuardDuty di sicurezza

È possibile gestire il GuardDuty security agent per la risorsa che si desidera monitorare. Se desideri monitorare più di un tipo di risorsa, assicurati di gestire l' GuardDuty agente per quella risorsa.

I seguenti argomenti ti aiuteranno nei passaggi successivi per gestire il Security Agent.

Indice

- [Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2](#)
- [Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2](#)
- [Gestione dell'agente di sicurezza automatizzato per Fargate \(solo Amazon ECS\)](#)
- [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)
- [Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS](#)
- [Configurazione GuardDuty dei parametri dell'agente di sicurezza \(componente aggiuntivo\) per Amazon EKS](#)
- [Convalida della configurazione degli endpoint VPC](#)

Abilitazione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2

Questa sezione include i passaggi per abilitare l'agente GuardDuty automatizzato per le tue risorse Amazon EC2 nel tuo account autonomo o in un ambiente con più account.

Prima di continuare, assicurati di seguire tutte le. [Prerequisiti per il supporto delle istanze Amazon EC2](#)

Se stai passando dalla gestione manuale dell' GuardDuty agente all'attivazione dell'agente GuardDuty automatizzato, prima di seguire i passaggi per abilitare l'agente GuardDuty automatizzato, consulta [Migrazione dall'agente manuale di Amazon EC2 all'agente automatizzato](#).

GuardDuty Agente di abilitazione per le risorse Amazon EC2 in un ambiente con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatica degli agenti per i tipi di risorse appartenenti agli account dei membri dell'organizzazione. GuardDuty Gli account membro non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta [Gestione di più account](#).

Per l'account amministratore delegato GuardDuty

Configure for all instances

Se hai scelto Abilita per tutti gli account per il monitoraggio del runtime, scegli una delle seguenti opzioni per l'account GuardDuty amministratore delegato:

- Opzione 1

In Configurazione automatica dell'agente, nella sezione EC2, seleziona Abilita per tutti gli account.

- Opzione 2

- In Configurazione automatizzata dell'agente, nella sezione EC2, seleziona Configura gli account manualmente.

- In Amministratore delegato (questo account), scegli Abilita.

- Scegli Save (Salva).

Se hai scelto Configura gli account manualmente per il monitoraggio del runtime, procedi nel seguente modo:

- In Configurazione automatizzata degli agenti, nella sezione EC2, seleziona Configura gli account manualmente.

- In Amministratore delegato (questo account), scegli Abilita.
- Scegli Save (Salva).

Indipendentemente dall'opzione scelta per abilitare la configurazione automatica dell'agente per l'account GuardDuty amministratore delegato, puoi verificare che l'associazione SSM GuardDuty creata installerà e gestirà il security agent su tutte le risorse EC2 appartenenti a questo account.

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Apri la scheda Targets per l'associazione SSM (GuardDutyRuntimeMonitoring-do-not-delete). Osservate che il tasto Tag appare come Instancelds.

Using inclusion tag in selected instances

Per configurare GuardDuty l'agente per istanze Amazon EC2 selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il true tagGuardDutyManaged: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).

L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze EC2 selezionate. Non è necessario abilitare la configurazione automatica degli agenti in modo esplicito.

3. È possibile verificare che l'associazione SSM GuardDuty creata installi e gestisca il security agent solo sulle risorse EC2 etichettate con i tag di inclusione.

Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>

- Apri la scheda Target per l'associazione SSM che viene creata (GuardDutyRuntimeMonitoring-do-not-delete). La chiave Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

Note

Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare GuardDuty l'agente per istanze Amazon EC2 selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `false` tagGuardDutyManaged: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).
3. Affinché i [tag di esclusione siano disponibili](#) nei metadati dell'istanza, effettuate le seguenti operazioni:
 - a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.
 - b. Nel menu Azioni, scegli Impostazioni istanza.
 - c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. [Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2](#)

Attivazione automatica per tutti gli account dei membri

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Configure for all instances

I passaggi seguenti presuppongono che tu abbia scelto Abilita per tutti gli account nella sezione Runtime Monitoring:

1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica degli agenti per Amazon EC2.
2. Puoi verificare che l'associazione SSM che GuardDuty crea (GuardDutyRuntimeMonitoring-do-not-delete) installi e gestisca il security agent su tutte le risorse EC2 appartenenti a questo account.
 - a. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
 - b. Apri la scheda Target per l'associazione SSM. Osserva che il tasto Tag appare come Instancelds.

Using inclusion tag in selected instances

Per configurare GuardDuty l'agente per istanze Amazon EC2 selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il true tagGuardDutyManaged: alle istanze EC2 che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Aggiungere un tag a una singola risorsa](#).

L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze EC2 selezionate. Non è necessario abilitare la configurazione automatica degli agenti in modo esplicito.

3. Puoi verificare che l'associazione SSM che GuardDuty crea installerà e gestirà il security agent su tutte le risorse EC2 appartenenti al tuo account.

- a. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
- b. Apri la scheda Targets per l'associazione SSM (GuardDutyRuntimeMonitoring-donot-delete). Osservate che il tasto Tag appare come Instancelds.

Using exclusion tag in selected instances

Note

Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente GuardDuty di sicurezza per istanze Amazon EC2 selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il false tagGuardDutyManaged: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).
3. Affinché i [tag di esclusione siano disponibili](#) nei metadati dell'istanza, effettuate le seguenti operazioni:
 - a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.
 - b. Nel menu Azioni, scegli Impostazioni istanza.
 - c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. [Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2](#)

Attivazione automatica solo per gli account dei nuovi membri

L'account GuardDuty amministratore delegato può impostare la configurazione automatica dell'agente per la risorsa Amazon EC2 in modo che si abiliti automaticamente per i nuovi account membri quando entrano a far parte dell'organizzazione.

Configure for all instances

I passaggi seguenti presuppongono che tu abbia selezionato Abilita automaticamente gli account dei nuovi membri nella sezione Runtime Monitoring:

1. Nel riquadro di navigazione, scegli Runtime Monitoring.
2. Nella pagina Runtime Monitoring, scegli Modifica.
3. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, la configurazione automatizzata degli agenti per Amazon EC2 venga abilitata automaticamente per l'account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa selezione.
4. Scegli Save (Salva).

Quando un nuovo account membro si unisce all'organizzazione, questa configurazione verrà abilitata automaticamente per lui. GuardDuty Per gestire l'agente di sicurezza per le istanze Amazon EC2 che appartengono a questo nuovo account membro, assicurati che tutti i prerequisiti [Per l'istanza EC2](#) siano soddisfatti.

Quando viene creata un'associazione SSM (GuardDutyRuntimeMonitoring-do-not-delete), puoi verificare che l'associazione SSM installi e gestisca il security agent su tutte le istanze EC2 appartenenti al nuovo account membro.

- Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
- Apri la scheda Target per l'associazione SSM. Osserva che il tasto Tag appare come Instancelds.

Using inclusion tag in selected instances

Per configurare il GuardDuty Security Agent per istanze selezionate nel tuo account

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `true` tagGuardDutyManaged: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).

L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze selezionate. Non è necessario abilitare esplicitamente la configurazione automatica dell'agente.

3. È possibile verificare che l'associazione SSM GuardDuty creata installi e gestisca il security agent solo sulle risorse EC2 etichettate con i tag di inclusione.
 - a. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
 - b. Apri la scheda Target per l'associazione SSM che viene creata. La chiave Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

Note

Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare il GuardDuty Security Agent per istanze specifiche nel tuo account autonomo

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `false` tagGuardDutyManaged: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).

3. Affinché i [tag di esclusione siano disponibili](#) nei metadati dell'istanza, effettuate le seguenti operazioni:
 - a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.
 - b. Nel menu Azioni, scegli Impostazioni istanza.
 - c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. [Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2](#)

Solo account membri selettivi

Configure for all instances

1. Nella pagina Account, seleziona uno o più account per i quali desideri abilitare la configurazione dell'agente Runtime Monitoring-Automated (Amazon EC2). Assicurati che gli account selezionati in questo passaggio abbiano già abilitato il Runtime Monitoring.
2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di Runtime Monitoring-Automated (Amazon EC2).
3. Scegli Conferma.

Using inclusion tag in selected instances

Per configurare l'agente di GuardDuty sicurezza per istanze selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `true` tagGuardDutyManaged: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).

L'aggiunta di questo tag consentirà di GuardDuty gestire l'agente di sicurezza per le istanze Amazon EC2 con tag. Non è necessario abilitare esplicitamente la configurazione automatica degli agenti (Runtime Monitoring - Automated agent configuration (EC2)).

Using exclusion tag in selected instances

Note

Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente di GuardDuty sicurezza per istanze selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `false` tagGuardDutyManaged: alle istanze EC2 che non desideri GuardDuty monitorare o rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Aggiungere un tag a una singola risorsa](#).
3. Affinché i [tag di esclusione siano disponibili](#) nei metadati dell'istanza, effettuate le seguenti operazioni:
 - a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.
 - b. Nel menu Azioni, scegli Impostazioni istanza.
 - c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare. [Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2](#)

Abilitazione dell'agente GuardDuty automatizzato per le risorse Amazon EC2 in un account autonomo

A un account indipendente spetta la decisione di abilitare o disabilitare un piano di protezione Account AWS in uno specifico account. Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione del monitoraggio del runtime per ambienti con più account](#).

Dopo aver abilitato il Runtime Monitoring, assicurati GuardDuty di installare Security Agent tramite la configurazione automatica o la distribuzione manuale. Come parte del completamento di tutti i passaggi elencati nella procedura seguente, assicuratevi di installare il security agent.

In base alla tua preferenza di monitorare tutte le risorse Amazon EC2 o solo alcune, scegli un metodo preferito e segui i passaggi indicati nella tabella seguente.

Configure for all instances

Per configurare il monitoraggio del runtime per tutte le istanze nel tuo account autonomo

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Modifica.
4. Nella sezione EC2, scegli Abilita.
5. Scegli Save (Salva).
6. Puoi verificare che l'associazione SSM che GuardDuty crea installerà e gestirà il security agent su tutte le risorse EC2 appartenenti al tuo account.
 - a. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
 - b. Apri la scheda Targets per l'associazione SSM (GuardDutyRuntimeMonitoring-do-not-delete). Osservate che il tasto Tag appare come Instancelds.

Using inclusion tag in selected instances

Per configurare l'agente GuardDuty di sicurezza per istanze Amazon EC2 selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `true` tagGuardDutyManaged: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).
3. Puoi verificare che l'associazione SSM che GuardDuty crea installerà e gestirà il security agent solo sulle risorse EC2 etichettate con i tag di inclusione.

Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>

- Apri la scheda Target per l'associazione SSM che viene creata (GuardDutyRuntimeMonitoring-do-not-delete). La chiave Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

Note

Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente GuardDuty di sicurezza per istanze Amazon EC2 selezionate

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Aggiungi il `false` tagGuardDutyManaged: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta [Per aggiungere un tag a una singola risorsa](#).

3. Affinché i [tag di esclusione siano disponibili](#) nei metadati dell'istanza, effettuate le seguenti operazioni:
 - a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.
 - b. Seleziona l'istanza per la quale desideri consentire i tag.
 - c. Nel menu Azioni, scegli Impostazioni istanza.
 - d. Scegli Consenti tag nei metadati dell'istanza.
 - e. In Accesso ai tag nei metadati dell'istanza, seleziona Consenti.
 - f. Scegli Save (Salva).
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. [Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2](#)

Migrazione dall'agente manuale di Amazon EC2 all'agente automatizzato

Questa sezione si applica a Account AWS chi in precedenza gestiva manualmente il Security Agent e ora desidera utilizzare la configurazione GuardDuty automatizzata dell'agente. Se ciò non ti riguarda, continua con la configurazione del security agent per il tuo account.

Quando abiliti l'agente GuardDuty automatizzato, GuardDuty gestisce l'agente di sicurezza per tuo conto. Per informazioni sui passaggi GuardDuty necessari, consulta [Utilizza la configurazione automatica degli agenti \(scelta consigliata\)](#).

Eseguire la pulizia delle risorse

Eliminare l'associazione SSM

- Elimina qualsiasi associazione SSM che potresti aver creato durante la gestione manuale del security agent per Amazon EC2. Per ulteriori informazioni, consulta [Eliminazione](#) delle associazioni.
- Questo viene fatto in modo che GuardDuty possa assumere il controllo della gestione delle azioni SSM indipendentemente dal fatto che si utilizzino agenti automatici a livello di account o

di istanza (utilizzando tag di inclusione o esclusione). Per ulteriori informazioni su cosa possono essere eseguite le azioni SSM, GuardDuty consulta [Autorizzazioni di ruolo collegate al servizio per GuardDuty](#)

- Quando si elimina un'associazione SSM creata in precedenza per la gestione manuale del Security Agent, potrebbe verificarsi un breve periodo di sovrapposizione quando si GuardDuty crea un'associazione SSM per la gestione automatica del Security Agent. Durante questo periodo, potrebbero verificarsi conflitti basati sulla pianificazione SSM. Per ulteriori informazioni, consulta la pianificazione [SSM di Amazon EC2](#).

Gestisci i tag di inclusione ed esclusione per le tue istanze Amazon EC2

- Tag di inclusione: quando non abiliti la configurazione GuardDuty automatizzata degli agenti ma contrassegni una qualsiasi delle tue istanze Amazon EC2 con un tag di inclusione (`GuardDutyManaged:true`), GuardDuty crea un'associazione SSM che installerà e gestirà il security agent sulle istanze EC2 selezionate. Si tratta di un comportamento previsto che ti aiuta a gestire il security agent solo su istanze EC2 selezionate. Per ulteriori informazioni, consulta [Come funziona il monitoraggio del runtime con le istanze Amazon EC2](#).

Per GuardDuty impedire l'installazione e la gestione del security agent, rimuovi il tag di inclusione da queste istanze EC2. Per ulteriori informazioni, consulta [Aggiungere ed eliminare tag](#) nella Guida per l'utente di Amazon EC2.

- Tag di esclusione: se desideri abilitare la configurazione GuardDuty automatica degli agenti per tutte le istanze EC2 del tuo account, assicurati che nessuna istanza EC2 sia contrassegnata con un tag di esclusione (:). `GuardDutyManaged false`

Gestione manuale dell'agente di sicurezza per la risorsa Amazon EC2

Questa sezione fornisce i passaggi per installare e aggiornare manualmente l'agente di sicurezza per le risorse Amazon EC2.

Dopo aver abilitato il Runtime Monitoring, dovrai installare il GuardDuty security agent manualmente. Per gestire manualmente il GuardDuty security agent, devi prima creare manualmente un endpoint Amazon VPC. Dopodiché, puoi installare il security agent in modo GuardDuty che inizi a ricevere gli eventi di runtime dalle istanze Amazon EC2. Quando GuardDuty rilascia una nuova versione dell'agente per questa risorsa, puoi aggiornare la versione dell'agente nel tuo account.

I seguenti argomenti includono i passaggi per gestire continuamente l'agente di sicurezza per le tue risorse Amazon EC2.

Argomenti

- [Prerequisito: creazione manuale di un endpoint Amazon VPC](#)
- [Installazione manuale del security agent](#)
- [Aggiornamento manuale del GuardDuty security agent per l'istanza Amazon EC2](#)

Prerequisito: creazione manuale di un endpoint Amazon VPC

Prima di poter installare il GuardDuty security agent, devi creare un endpoint Amazon Virtual Private Cloud (Amazon VPC). Questo ti aiuterà a GuardDuty ricevere gli eventi di runtime delle tue istanze Amazon EC2.

Note

Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint VPC.

Per creare un endpoint Amazon VPC

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. <https://console.aws.amazon.com/vpc/>
2. Nel pannello di navigazione, in VPC private cloud, scegli Endpoints.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nella pagina Crea endpoint per Categoria servizio, scegli Altri servizi endpoint.
5. Per Nome servizio, inserisci **com.amazonaws.us-east-1.guardduty-data**.

Assicurati di sostituirlo **us-east-1** con il tuo. Regione AWS Questa deve essere la stessa regione dell'istanza Amazon EC2 che appartiene all'ID del tuo AWS account.

6. Scegli Verifica del servizio.
7. Dopo aver verificato con successo il nome del servizio, scegli il VPC in cui risiede l'istanza. Aggiungi la seguente policy per limitare l'utilizzo degli endpoint Amazon VPC solo all'account specificato. Con la Condition dell'organizzazione fornita sotto a questa policy, puoi aggiornare la policy seguente per limitare l'accesso all'endpoint. Per fornire il supporto degli endpoint Amazon VPC a un account specifico della tua organizzazione, IDs consulta. [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 account di `aws:PrincipalAccount` deve corrispondere all'account contenente il VPC e l'endpoint VPC. L'elenco seguente mostra come condividere l'endpoint VPC con altri account: AWS IDs

- Per specificare più account per accedere all'endpoint VPC, sostituisilo `"aws:PrincipalAccount": "111122223333"` con il seguente blocco:

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
]
```

Assicurati di sostituire l' AWS account IDs con l'account IDs di quegli account che devono accedere all'endpoint VPC.

- Per consentire a tutti i membri di un'organizzazione di accedere all'endpoint VPC, sostituiscilo "aws:PrincipalAccount": "**111122223333**" con la seguente riga:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

Assicurati di sostituire l'organizzazione **o-abcdef0123** con il tuo ID dell'organizzazione.

- Per limitare l'accesso a una risorsa tramite un ID dell'organizzazione, aggiungi il tuo ResourceOrgID alla politica. Per ulteriori informazioni, consulta la sezione [aws:ResourceOrgID](#) nella Guida per l'utente di IAM.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. In Impostazioni aggiuntive, scegli Abilita nome DNS.
9. In Sottoreti, scegli le sottoreti in cui risiede l'istanza.
10. In Gruppi di sicurezza, scegli un gruppo di sicurezza con la porta in ingresso 443 abilitata dal tuo VPC (o dalla tua istanza Amazon EC2). Se non disponi già di un gruppo di sicurezza con una porta in ingresso 443 abilitata, consulta [Creare un gruppo di sicurezza per il tuo VPC nella Amazon VPC User Guide](#).

Se c'è un problema durante la limitazione delle autorizzazioni in ingresso al tuo VPC (o istanza), puoi utilizzare la porta 443 in ingresso da qualsiasi indirizzo IP. (0.0.0.0/0) Tuttavia, GuardDuty consiglia di utilizzare indirizzi IP che corrispondano al blocco CIDR per il VPC. Per ulteriori informazioni, consulta i [blocchi VPC CIDR](#) nella Amazon VPC User Guide.

Dopo aver seguito i passaggi, verifica [Convalida della configurazione degli endpoint VPC](#) che l'endpoint VPC sia stato configurato correttamente.

Installazione manuale del security agent

GuardDuty fornisce i due metodi seguenti per installare il GuardDuty security agent sulle istanze Amazon EC2. Prima di procedere, assicurati di seguire i passaggi riportati di seguito. [Prerequisito: creazione manuale di un endpoint Amazon VPC](#)

Scegli un metodo di accesso preferito per installare il security agent nelle tue risorse Amazon EC2.

- [Metodo 1 - Utilizzo AWS Systems Manager](#)— Questo metodo richiede la gestione dell'istanza Amazon EC2. AWS Systems Manager

- [Metodo 2: utilizzo dei gestori di pacchetti Linux](#)— Puoi utilizzare questo metodo indipendentemente dal fatto che le tue istanze Amazon EC2 siano gestite o meno. AWS Systems Manager In base alle [distribuzioni del sistema operativo](#), è possibile scegliere un metodo appropriato per installare gli script RPM o gli script Debian. Se si utilizza la piattaforma Fedora, è necessario utilizzare questo metodo per installare l'agente.

Metodo 1 - Utilizzo AWS Systems Manager

Per utilizzare questo metodo, assicurati che le tue istanze Amazon EC2 siano AWS Systems Manager gestite, quindi installa l'agente.

AWS Systems Manager istanza Amazon EC2 gestita

Utilizza i seguenti passaggi per gestire le tue istanze AWS Systems Manager Amazon EC2.

- [AWS Systems Manager](#) ti aiuta a gestire AWS applicazioni e risorse end-to-end e a consentire operazioni sicure su larga scala.

Per gestire le istanze Amazon EC2 con AWS Systems Manager, consulta [Configurazione delle istanze di Systems Manager per Amazon EC2 nella Guida per l'utente](#). AWS Systems Manager

- La tabella seguente mostra i nuovi documenti gestiti: GuardDuty AWS Systems Manager

Nome del documento	Tipo di documento	Scopo
AmazonGuardDuty-RunTimeMonitoringSsmPlugin	Distributore	Per impacchettare il GuardDuty security agent.
AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin	Comando	Per eseguire lo script di installazione/disinstallazione per installare il security agent. GuardDuty

Per ulteriori informazioni AWS Systems Manager, consulta i documenti di [Amazon EC2 Systems Manager](#) nella Guida per AWS Systems Manager l'utente.

Per i server Debian

L'Amazon Machine Images (AMIs) per Debian Server fornito da AWS richiede l'installazione dell' AWS Systems Manager agente (agente SSM). È necessario eseguire un passaggio aggiuntivo per installare l'agente SSM per gestire le istanze di Amazon EC2 Debian Server tramite SSM. Per informazioni sui passaggi da eseguire, vedere [Installazione manuale dell'agente SSM sulle istanze del server Debian](#) nella Guida per l'utente.AWS Systems Manager

Per installare l' GuardDuty agente per l'istanza Amazon EC2 utilizzando AWS Systems Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, scegli Documenti
3. In Owned by Amazon, scegliAmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
4. Scegliere Run Command.
5. Inserisci i seguenti parametri Run Command
 - Azione: Scegli Installa.
 - Tipo di installazione: scegli Installa o Disinstalla.
 - Valore: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
 - Versione: se rimane vuoto, otterrai la versione più recente del GuardDuty Security Agent. Per ulteriori informazioni sulle versioni di rilascio,[GuardDuty versioni degli agenti di sicurezza per le istanze Amazon EC2](#).
6. Seleziona l'istanza Amazon EC2 di destinazione. Puoi selezionare una o più istanze Amazon EC2. Per ulteriori informazioni, consulta [AWS Systems Manager Esecuzione di comandi dalla console nella Guida](#) per l'AWS Systems Manager utente
7. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni, consulta [Convalida dello stato di installazione del GuardDuty Security Agent](#).

Metodo 2: utilizzo dei gestori di pacchetti Linux

Con questo metodo, è possibile installare l'agente GuardDuty di sicurezza eseguendo script RPM o script Debian. In base ai sistemi operativi, puoi scegliere un metodo preferito:

- Usa gli script RPM per installare il security agent su distribuzioni OS AL2 AL2023, RedHat CentOS o Fedora.
- Usa gli script Debian per installare il security agent sulle distribuzioni del sistema operativo Ubuntu o Debian. Per informazioni sulle distribuzioni supportate di Ubuntu e Debian OS, vedere. [Convalida i requisiti architetturici](#)

RPM installation

Important

Si consiglia di verificare la firma RPM del GuardDuty Security Agent prima di installarla sulla macchina.

1. Verifica la firma RPM del GuardDuty Security Agent

a. Preparare il modello

Prepara i comandi con la chiave pubblica appropriata, la firma di x86_64 RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli script RPM ospitati nei bucket Amazon S3. Sostituisci il valore dell'ID dell' AWS account e la versione dell' Regione AWS agente per accedere agli script RPM. GuardDuty

- Chiave pubblica:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/publickey.pem
```

- GuardDuty firma RPM dell'agente di sicurezza:

Firma di x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/x86_64/amazon-guardduty-agent-1.9.2.x86_64.sig
```

Firma di arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/arm64/
amazon-guardduty-agent-1.9.2.arm64.sig
```

- Accedi ai link agli script RPM nel bucket Amazon S3:

Link di accesso per x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/x86_64/
amazon-guardduty-agent-1.9.2.x86_64.rpm
```

Link di accesso per arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/arm64/
amazon-guardduty-agent-1.9.2.arm64.rpm
```

Regione AWS	Nome della Regione	AWS ID dell'account
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Stati Uniti orientali (Virginia settentrionale)	593207742271
us-west-2	Stati Uniti occidentali (Oregon)	733349766148
eu-west-3	Europa (Parigi)	665651866788
us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381

me-south-1	Medio Oriente (Bahrein)	536382113932
eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834
ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217
sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente (Emirati Arabi Uniti)	000014521398
us-west-1	Stati Uniti occidentali (California settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469
ca-west-1	Canada occidentale (Calgary)	339712888787
ap-south-2	Asia Pacifico (Hyderabad)	950823858135
eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535

ap-southeast-7	Asia Pacifico (Thailandia)	054037130133
il-central-1	Israele (Tel Aviv)	870907303882
mx-central-1	Messico (centrale)	982081086614
ap-east-2	Asia Pacifico (Taipei)	259886477082

b. Scarica il modello

Nel seguente comando per scaricare la chiave pubblica appropriata, la firma di x86_64 RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli script RPM ospitati nei bucket Amazon S3, assicurati di sostituire l'ID dell'account con l'ID appropriato e la regione con la regione corrente. Account AWS

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/
x86_64/amazon-guardduty-agent-1.9.2.x86_64.rpm ./amazon-guardduty-
agent-1.9.2.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/
x86_64/amazon-guardduty-agent-1.9.2.x86_64.sig ./amazon-guardduty-
agent-1.9.2.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.2/
publickey.pem ./publickey.pem
```

c. Importa la chiave pubblica

Usa il seguente comando per importare la chiave pubblica nel database:

```
gpg --import publickey.pem
```

gpg mostra l'importazione con successo

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Verifica la firma

Utilizzate il seguente comando per verificare la firma

```
gpg --verify amazon-guardduty-agent-1.9.2.x86_64.sig amazon-guardduty-agent-1.9.2.x86_64.rpm
```

Se la verifica ha esito positivo, verrà visualizzato un messaggio simile al risultato riportato di seguito. È ora possibile procedere all'installazione del GuardDuty security agent utilizzando RPM.

Output di esempio:

```
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
```

Se la verifica fallisce, significa che la firma su RPM è stata potenzialmente manomessa. È necessario rimuovere la chiave pubblica dal database e ripetere il processo di verifica.

Esempio:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Usa il seguente comando per rimuovere la chiave pubblica dal database:

```
gpg --delete-keys AwsGuardDuty
```

Ora prova di nuovo la procedura di verifica.

2. [Connect con SSH da Linux o macOS.](#)
3. Installa il GuardDuty security agent utilizzando il seguente comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.9.2.x86_64.rpm
```

4. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni sui passaggi, vedere [Convalida dello stato di installazione del GuardDuty Security Agent.](#)

Debian installation

Important

Si consiglia di verificare la firma Debian del GuardDuty security agent prima di installarla sulla macchina.

1. Verifica la firma Debian dell'agente GuardDuty di sicurezza
 - a. Preparare i modelli per la chiave pubblica appropriata, la firma del pacchetto Debian amd64, la firma del pacchetto Debian arm64 e il collegamento di accesso corrispondente agli script Debian ospitati nei bucket Amazon S3

Nei seguenti modelli, sostituisci il valore di Regione AWS, AWS account ID e la versione dell'agente per accedere agli script dei GuardDuty pacchetti Debian.

- Chiave pubblica:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/publickey.pem
```

- GuardDuty firma Debian dell'agente di sicurezza:

Firma di amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/amd64/amazon-guardduty-agent-1.9.2.amd64.sig
```

Firma di arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/arm64/amazon-guardduty-agent-1.9.2.arm64.sig
```

- Accedi ai link agli script Debian nel bucket Amazon S3:

Link di accesso per amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/amd64/amazon-guardduty-agent-1.9.2.amd64.deb
```


Link di accesso per arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/arm64/
amazon-guardduty-agent-1.9.2.arm64.deb
```

Regione AWS	Nome della Regione	AWS ID dell'account
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Stati Uniti orientali (Virginia settentrionale)	593207742271
us-west-2	Stati Uniti occidentali (Oregon)	733349766148
eu-west-3	Europa (Parigi)	665651866788
us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Bahrein)	536382113932
eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834
ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217

sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente (Emirati Arabi Uniti)	000014521398
us-west-1	Stati Uniti occidentali (California settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469
ca-west-1	Canada occidentale (Calgary)	339712888787
ap-south-2	Asia Pacifico (Hyderabad)	950823858135
eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535
il-central-1	Israele (Tel Aviv)	870907303882
mx-central-1	Messico (centrale)	982081086614
ap-east-2	Asia Pacifico (Taipei)	259886477082

- b. Scarica la chiave pubblica appropriata, la firma di amd64, la firma di arm64 e il link di accesso corrispondente agli script Debian ospitati nei bucket Amazon S3

Nei seguenti comandi, sostituisci l'ID dell'account con l' Account AWS ID appropriato e la regione con la regione corrente.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/
amd64/amazon-guardduty-agent-1.9.2.amd64.deb ./amazon-guardduty-
agent-1.9.2.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/
amd64/amazon-guardduty-agent-1.9.2.amd64.sig ./amazon-guardduty-
agent-1.9.2.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.2/
publickey.pem ./publickey.pem
```

c. Importa la chiave pubblica nel database

```
gpg --import publickey.pem
```

gpg mostra che l'importazione è avvenuta con successo

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Verifica la firma

```
gpg --verify amazon-guardduty-agent-1.9.2.amd64.sig amazon-guardduty-
agent-1.9.2.amd64.deb
```

Dopo una verifica avvenuta con successo, vedrai un messaggio simile al seguente risultato:

Output di esempio:

```
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
```

È ora possibile procedere all'installazione del GuardDuty security agent utilizzando Debian.

Tuttavia, se la verifica fallisce, significa che la firma nel pacchetto Debian è stata potenzialmente manomessa.

Esempio:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Usare il seguente comando per rimuovere la chiave pubblica dal database:

```
gpg --delete-keys AwsGuardDuty
```

Ora, riprova il processo di verifica.

2. [Connect con SSH da Linux o macOS.](#)
3. Installa il GuardDuty security agent utilizzando il seguente comando:

```
sudo dpkg -i amazon-guardduty-agent-1.9.2.amd64.deb
```

4. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni sui passaggi, vedere [Convalida dello stato di installazione del GuardDuty Security Agent.](#)

Errore di memoria esaurita

Se riscontri un out-of-memory errore durante l'installazione o l'aggiornamento manuale del GuardDuty Security Agent per Amazon EC2, consulta. [Risoluzione dell'errore di esaurimento della memoria](#)

Convalida dello stato di installazione del GuardDuty Security Agent

Dopo aver eseguito i passaggi per installare il GuardDuty security agent, utilizzate i seguenti passaggi per convalidare lo stato dell'agente:

Per verificare se il GuardDuty security agent è integro

1. [Connect con SSH da Linux o macOS.](#)
2. Esegui il comando seguente per verificare lo stato del GuardDuty security agent:

```
sudo systemctl status amazon-guardduty-agent
```

Se desideri visualizzare i registri di installazione del Security Agent, sono disponibili in `/var/log/amzn-guardduty-agent/`.

Per visualizzare i log, fai. `sudo journalctl -u amazon-guardduty-agent`

Aggiornamento manuale del GuardDuty security agent per l'istanza Amazon EC2

GuardDuty rilascia aggiornamenti alle versioni del Security Agent. Quando gestisci manualmente l'agente di sicurezza, sei responsabile dell'aggiornamento dell'agente per le tue istanze Amazon EC2. Per informazioni sulle nuove versioni degli agenti, consulta [GuardDuty versioni di rilascio di Security Agent](#) per le istanze Amazon EC2. Per ricevere notifiche relative al rilascio di una nuova versione dell'agente, consulta. [Iscrizione agli annunci di Amazon SNS GuardDuty](#)

Per aggiornare manualmente l'agente di sicurezza per l'istanza Amazon EC2

Il processo di aggiornamento del security agent è lo stesso dell'installazione del security agent. A seconda del metodo utilizzato per installare l'agente, puoi eseguire i passaggi [Installazione manuale del security agent](#) per le istanze Amazon EC2.

Se utilizzi [Method 1 - By using AWS Systems Manager](#), puoi aggiornare il security agent utilizzando il comando Run. Utilizza la versione dell'agente a cui desideri eseguire l'aggiornamento.

Se si utilizza [il Metodo 2 - Utilizzando Linux Package Managers](#), è possibile utilizzare gli script come specificato nella [Installazione manuale del security agent](#) sezione. Gli script includono già l'ultima versione rilasciata dall'agente. Per informazioni sulle versioni dell'agente rilasciate di recente, vedere [GuardDuty versioni degli agenti di sicurezza per le istanze Amazon EC2](#).

Dopo aver aggiornato il Security Agent, puoi controllare lo stato dell'installazione esaminando i log. Per ulteriori informazioni, consulta [Convalida dello stato di installazione del GuardDuty Security Agent](#).

Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)

Runtime Monitoring supporta la gestione dell'agente di sicurezza per i cluster Amazon ECS (AWS Fargate) solo tramite. GuardDuty Non è disponibile alcun supporto per la gestione manuale del security agent sui cluster Amazon ECS.

Prima di procedere con i passaggi di questa sezione, assicurati di seguire. [Prerequisiti per il AWS Fargate supporto \(solo Amazon ECS\)](#)

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nelle risorse di Amazon ECS-Fargate](#), scegli un metodo preferito per abilitare l'agente GuardDuty automatizzato per le tue risorse.

Configurazione GuardDuty dell'agente per un ambiente con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatica degli agenti per gli account dei membri e gestire la configurazione automatizzata degli agenti per i cluster Amazon ECS che appartengono agli account dei membri della loro organizzazione. Un account GuardDuty membro non può modificare questa configurazione. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti con più account, vedere [Gestione di più account](#) in. GuardDuty

Abilitazione della configurazione automatizzata degli agenti per l'account amministratore delegato GuardDuty

Manage for all Amazon ECS clusters (account level)

Se hai scelto Abilita per tutti gli account per il monitoraggio del runtime, hai le seguenti opzioni:

- Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà l'agente di sicurezza per tutte le attività di Amazon ECS che verranno lanciate.
- Scegli Configura gli account manualmente.

Se hai scelto Configura gli account manualmente nella sezione Runtime Monitoring, procedi come segue:

1. Scegli Configura gli account manualmente nella sezione Configurazione automatica degli agenti.
2. Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).

Scegli Save (Salva).

Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione

per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -.
GuardDutyManaged false
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
- 5.

 Note

Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

Nella scheda Configurazione, scegli Abilita nella configurazione automatizzata dell'agente.

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

6. Scegli Save (Salva).
7. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. GuardDutyManaged true
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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

Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente GuardDuty l'agente tramite la configurazione automatica degli agenti.

3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Attivazione automatica per tutti gli account dei membri

Manage for all Amazon ECS clusters (account level)

I passaggi seguenti presuppongono che tu abbia scelto Abilita per tutti gli account nella sezione Runtime Monitoring.

1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà l'agente di sicurezza per tutte le attività di Amazon ECS che verranno lanciate.
2. Scegli Save (Salva).
3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -.
GuardDutyManaged false
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

4. Nel pannello di navigazione, scegli Runtime Monitoring.

5.

 Note

Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

Nella scheda Configurazione, scegli Modifica.

6. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

7. Scegli Save (Salva).

8. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Indipendentemente da come scegli di abilitare il Runtime Monitoring, i seguenti passaggi ti aiuteranno a monitorare attività selettive di Amazon ECS Fargate per tutti gli account membri della tua organizzazione.

1. Non abilitare alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella selezionata nel passaggio precedente.
2. Scegli Save (Salva).
3. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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

Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la gestione automatica degli GuardDuty agenti.

4. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Abilitazione della configurazione automatica degli agenti per gli account dei membri attivi esistenti

Manage for all Amazon ECS clusters (account level)

1. Nella pagina Runtime Monitoring, nella scheda Configurazione, è possibile visualizzare lo stato corrente della configurazione automatizzata dell'agente.
2. Nel riquadro di configurazione dell'agente automatizzato, nella sezione Account membri attivi, scegli Azioni.
3. Da Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
4. Scegli Conferma.
5. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.

- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -.
GuardDutyManaged false
2. Impedisce la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in [Impedisce che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
- 5.

 Note

Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

Nella scheda Configurazione, nella sezione Configurazione automatizzata dell'agente, in Account membri attivi, scegli Azioni.

6. Da Operazioni, scegli Abilita per tutti gli account membri attivi.

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

7. Scegli Conferma.
8. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged true`

2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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

Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Abilita automaticamente la configurazione automatizzata degli agenti per i nuovi membri

Manage for all Amazon ECS clusters (account level)

1. Nella pagina Runtime Monitoring, scegli Modifica per aggiornare la configurazione esistente.
2. Nella sezione Configurazione automatizzata dell'agente, seleziona Abilita automaticamente per nuovi account membro.
3. Scegli Save (Salva).
4. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -.
`GuardDutyManaged false`

2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
- 5.

 Note

Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario,

il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

Nella scheda Configurazione, seleziona **Abilita automaticamente** gli account dei nuovi membri nella sezione Configurazione automatica degli agenti.

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

6. Scegli **Save** (Salva).
7. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere `- GuardDutyManaged true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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

Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

- Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Abilitazione selettiva della configurazione automatizzata degli agenti per gli account dei membri attivi

Manage for all Amazon ECS (account level)

1. Nella pagina Account, selezionare gli account per i quali si desidera abilitare la configurazione dell'agente Runtime Monitoring-Automated (ECS-Fargate). È possibile selezionare più account. Assicurati che gli account selezionati in questo passaggio siano già abilitati con Runtime Monitoring.
2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di monitoraggio del runtime (ECS-Fargate).
3. Scegli Conferma.
4. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come `GuardDutyManaged false`.
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
- 5.

 Note

Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

Nella pagina Account, selezionare gli account per i quali si desidera abilitare la configurazione dell'agente Runtime Monitoring-Automated (ECS-Fargate). È possibile selezionare più account. Assicurati che gli account selezionati in questo passaggio siano già abilitati con Runtime Monitoring.

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

6. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di monitoraggio del runtime (ECS-Fargate).
7. Scegli Save (Salva).
8. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Assicurati di non abilitare la configurazione automatizzata degli agenti (o la configurazione degli agenti automatizzati di Runtime Monitoring-ECS-Fargate) per gli account selezionati che hanno i cluster Amazon ECS che desideri monitorare.
2. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. GuardDutyManaged true
3. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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

Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

- Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.
- [update-service](#) nel AWS CLI Command Reference.

Configurazione dell' GuardDuty agente per un account autonomo

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione:
 - a. Per gestire la configurazione automatizzata degli agenti per tutti i cluster Amazon ECS (a livello di account)

Scegli Abilita nella sezione Configurazione automatica dell'agente per AWS Fargate (solo ECS). All'avvio di una nuova attività Fargate Amazon ECS, GuardDuty gestirà l'implementazione del security agent.

- Scegli Save (Salva).
- b. Per gestire la configurazione automatizzata degli agenti escludendo alcuni cluster Amazon ECS (a livello di cluster)
 - i. Aggiungi un tag al cluster Amazon ECS per il quale desideri escludere tutte le attività. La coppia chiave-valore deve essere -. GuardDutyManaged false
 - ii. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisci che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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. Nella scheda Configurazione, scegli Abilita nella sezione Configurazione automatica dell'agente.

 Note

Aggiungi sempre il tag di esclusione al tuo cluster Amazon ECS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, l'agente di sicurezza verrà distribuito in tutte le attività avviate all'interno del cluster Amazon ECS corrispondente.

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

- iv. Scegli Save (Salva).
- c. Per gestire la configurazione automatizzata degli agenti includendo alcuni cluster Amazon ECS (a livello di cluster)
 - i. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. GuardDutyManaged true
 - ii. Impedisce la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in [Impedisce che i tag vengano modificati se non in base ai principi autorizzati](#) nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

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
        }
    }
}
]
}

```

- Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un servizio ECS specifico è stata avviata prima di abilitare il Runtime Monitoring, puoi riavviare il servizio o aggiornarlo utilizzando `forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- [Aggiornamento di un servizio Amazon ECS utilizzando la console](#) nell'Amazon Elastic Container Service Developer Guide.
- [UpdateService](#) nel riferimento all'API di riferimento di Amazon Elastic Container Service.

- [update-service](#) nel AWS CLI Command Reference.

Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS

Il monitoraggio del runtime supporta l'abilitazione del security agent tramite configurazione GuardDuty automatizzata e manuale. Questa sezione fornisce i passaggi per abilitare la configurazione automatizzata degli agenti per i cluster Amazon EKS.

Prima di procedere, assicurati di aver seguito il [Prerequisiti per il supporto dei cluster Amazon EKS](#)

In base al tuo approccio preferito [Gestisci l'agente di sicurezza tramite GuardDuty](#), scegli di conseguenza i passaggi nelle sezioni seguenti.

Configurazione dell'agente automatizzato per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatizzata degli agenti per gli account dei membri e gestire l'agente automatizzato per i cluster EKS appartenenti agli account membro dell'organizzazione. GuardDuty Gli account dei membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta [Gestione di più account](#).

Configurazione della configurazione automatizzata dell'agente per l'account amministratore delegato GuardDuty

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	Se hai scelto Abilita per tutti gli account nella sezione Runtime Monitoring, hai le seguenti opzioni: • Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty implementerà e gestirà l'agente di sicurezza per tutti i cluster EKS che appartengono all'account GuardDuty amministratore delegato e anche per tutti i cluster EKS che appartengono a tutti gli account membro esistenti e potenzialmente nuovi dell'organizzazione.

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	• Scegli Configura gli account manualmente. Se hai scelto Configura gli account manualmente nella sezione Runtime Monitoring, procedi come segue: 1. Scegli Configura gli account manualmente nella sezione Configurazione automatica degli agenti. 2. Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account). Scegli Save (Salva).

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave GuardDuty Managed e il valore corrispondente false. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring.

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	 Note Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, l'agente GuardDuty di sicurezza verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, scegli Abilita nella sezione Gestione degli agenti. GuardDuty Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Scegli Save (Salva). Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave <code>GuardDutyManaged</code> e il valore corrispondente <code>false</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <code>ec2:CreateTags</code> con <code>eks:TagResource</code> . • Sostituisci <code>ec2:DeleteTags</code> con <code>eks:UntagResource</code> .

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	• Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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. Se l'agente automatizzato era abilitato per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring 4. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring consulta.

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi nel vostro account: 1. Assicurati di scegliere Disabilita per l'account GuardDuty amministratore delegato (questo account) nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Scegli Save (Salva). 3. Aggiungi un tag al cluster EKS con la chiave GuardDuty Managed e il valore corrispondente true. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn :

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	<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>
Gestisci manualmente l'agente di GuardDuty sicurezza	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, potete gestire manualmente il security agent per i vostri cluster EKS. 1. Assicurati di scegliere Disabilita per l'account GuardDuty amministratore delegato (questo account) nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Scegli Save (Salva). 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilita automaticamente l'agente automatizzato per tutti gli account dei membri

 Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty	Questo argomento riguarda l'abilitazione del monitoraggio del runtime per tutti gli account membri e, pertanto, i passaggi seguenti

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
(Monitorare tutti i cluster EKS)	presuppongono che sia necessario aver scelto Abilita per tutti gli account nella sezione Runtime Monitoring. 1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty implementerà e gestirà l'agente di sicurezza per tutti i cluster EKS che appartengono all'account GuardDuty amministratore delegato e anche per tutti i cluster EKS che appartengono a tutti gli account membro esistenti e potenzialmente nuovi dell'organizzazione. 2. Scegli Save (Salva).

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando l'agente GuardDuty di sicurezza non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave GuardDuty Managed e il valore corrispondente false. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	 Note Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare Automated Agent per il tuo account; in caso contrario, l'agente di GuardDuty sicurezza verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring. 6. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 7. Scegli Save (Salva). Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave GuardDuty Managed e il valore corrispondente false. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Se la configurazione automatizzata dell'agente era abilitata per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà l'agente di sicurezza per questo cluster. Tuttavia, l'agente di sicurezza rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> <code>GuardDutyManaged</code> • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più <code>PrincipalArn</code> : <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> 4. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi per tutti gli account membri della vostra organizzazione: 1. Non abilitate alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Scegli Save (Salva). 3. Aggiungi un tag al cluster EKS con la chiave GuardDuty Managed e il valore corrispondente true. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn :

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	<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>
Gestisci manualmente l'agente di GuardDuty sicurezza	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, potete gestire manualmente il security agent per i vostri cluster EKS. 1. Non abilitate alcuna configurazione nella sezione Configurazione automatizzata dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Scegli Save (Salva). 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Attivazione dell'agente automatizzato per tutti gli account dei membri attivi esistenti

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Per gestire il GuardDuty Security Agent per gli account dei membri attivi esistenti nell'organizzazione

- GuardDuty Per ricevere gli eventi di runtime dai cluster EKS che appartengono agli account dei membri attivi esistenti nell'organizzazione, è necessario scegliere un approccio preferito per gestire l'agente di GuardDuty sicurezza per questi cluster EKS. Per ulteriori informazioni su ognuno di questi approcci, consulta [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#).

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	Per monitorare tutti i cluster EKS per tutti gli account membri attivi esistenti 1. Nella pagina Runtime Monitoring, nella scheda Configurazione, è possibile visualizzare lo stato corrente della configurazione automatizzata dell'agente. 2. Nel riquadro di configurazione dell'agente automatizzato, nella sezione Account membri attivi, scegli Azioni. 3. Da Operazioni, scegli Abilita per tutti gli account membri attivi esistenti. 4. Scegli Conferma.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave <code>GuardDutyManaged</code> e il valore corrispondente <code>false</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <code>ec2:CreateTags</code> con <code>eks:TagResource</code> . • Sostituisci <code>ec2:DeleteTags</code> con <code>eks:UntagResource</code> . • Sostituisci con <code>access-project</code> GuardDuty Managed • Sostituisci <code>123456789012</code> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-</pre>

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	<pre>admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring.  Note Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, nel riquadro Configurazione automatizzata dell'agente, in Account membri attivi, scegli Azioni. 6. Da Operazioni, scegli Abilita per tutti gli account membri attivi. 7. Scegli Conferma. Per escludere un cluster EKS dal monitoraggio dopo che il GuardDuty security agent è già stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave GuardDutyManaged e il valore corrispondente false.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Dopo questo passaggio, non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDuty Managed • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:</pre>

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	<code>iam::123456789012:role/org-admins/iam-admin"]</code> 3. Indipendentemente dal modo in cui gestisci il security agent (tramite GuardDuty o manualmente), per interrompere la ricezione degli eventi di runtime da questo cluster, devi rimuovere il security agent distribuito da questo cluster EKS. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	1. Nella pagina Account, dopo aver abilitato Runtime Monitoring, non attivate Runtime Monitoring - Configurazione automatica dell'agente. 2. Aggiungi un tag al cluster EKS che appartiene all'account selezionato che desideri monitorare. La coppia chiave-valore del tag deve essere <code>GuardDutyManaged -true</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations. Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code>. • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code>. • Sostituisci con <i>access-project</i> GuardDuty Managed • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn :

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	<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>
Gestisci manualmente l'agente di GuardDuty sicurezza	1. Assicurati di non scegliere Abilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Scegli Save (Salva). 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilita automaticamente la configurazione automatica degli agenti per i nuovi membri

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	1. Nella pagina Runtime Monitoring, scegli Modifica per aggiornare la configurazione esistente. 2. Nella sezione Configurazione automatizzata dell'agente, seleziona Abilita automaticamente per nuovi account membro. 3. Scegli Save (Salva).
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave <code>GuardDutyManaged</code> e il valore corrispondente <code>false</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <code>ec2:CreateTags</code> con <code>eks:TagResource</code> . • Sostituisci <code>ec2:DeleteTags</code> con <code>eks:UntagResource</code> . • Sostituisci con <code>access-project</code> GuardDuty Managed • Sostituisci <code>123456789012</code> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più <code>PrincipalArn</code> : <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>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring.  Note Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, seleziona Abilita automaticamente gli account dei nuovi membri nella sezione Gestione degli GuardDuty agenti. Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Scegli Save (Salva). Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Indipendentemente dal fatto che gestiate il GuardDuty security agent tramite GuardDuty o manualmente, aggiungete un tag a questo cluster EKS con la chiave <code>as GuardDutyManaged</code> e il relativo valore. <code>false</code> Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Se l'agente automatizzato era abilitato per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà l'agente di sicurezza per questo cluster. Tuttavia, l'agente di sicurezza rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDuty Managed • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin</pre>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"] 3. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi per i nuovi account membro della vostra organizzazione. 1. Assicurati di deselezionare Abilita automaticamente per nuovi account membro nella sezione Configurazione automatica degli agenti. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Scegli Save (Salva). 3. Aggiungi un tag al cluster EKS con la chiave <code>GuardDutyManaged</code> e il valore corrispondente <code>true</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <code>ec2:CreateTags</code> con <code>eks:TagResource</code> . • Sostituisci <code>ec2:DeleteTags</code> con <code>eks:UntagResource</code> . • Sostituisci con <code>access-project</code> <code>GuardDutyManaged</code>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	• Sostituisci 123456789012 con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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>
Gestisci manualmente l'agente di GuardDuty sicurezza	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, potete gestire manualmente il security agent per i vostri cluster EKS. 1. Assicurati di deselezionare la casella di controllo Abilita automaticamente gli account dei nuovi membri nella sezione Configurazione automatica degli agenti. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Scegli Save (Salva). 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione selettiva dell'agente automatizzato per gli account dei membri attivi

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	1. Nella pagina Account, seleziona gli account per i quali desideri abilitare la configurazione automatica degli agenti. Puoi selezionare più di un account alla volta. Assicurati che il monitoraggio del runtime EKS sia già abilitato per gli account selezionati in questa fase. 2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare Runtime Monitoring - Configurazione automatica degli agenti. 3. Scegli Conferma.
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave GuardDuty Managed e il valore corrispondente false. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre data-bbox="618 428 1507 625">"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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.  Note Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. 4. Nella pagina Account, seleziona l'account per il quale desideri abilitare Gestisci automaticamente l'agente. Puoi selezionare più di un account alla volta. 5. Da Modifica piani di protezione, scegliete l'opzione appropriata per abilitare la configurazione automatica dell'agente di monitoraggio del runtime per l'account selezionato. Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent. GuardDuty 6. Scegli Save (Salva).

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster Aggiungi un tag a questo cluster EKS con la chiave GuardDuty Managed e il valore corrispondente false. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Se in precedenza era stata abilitata la configurazione dell'agente automatizzato per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, l'agente di sicurezza rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . - Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . - Sostituisci con <i>access-project</i> GuardDutyManaged - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre data-bbox="618 428 1507 625">"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. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, devi rimuoverlo. Per ulteriori informazioni, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi che appartengono agli account selezionati: 1. Assicuratevi di non abilitare la configurazione automatica degli agenti di Runtime Monitoring-Automated per gli account selezionati che dispongono dei cluster EKS che desiderate monitorare. 2. Aggiungi un tag al cluster EKS con la chiave GuardDuty Managed e il valore corrispondente true. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Dopo aver aggiunto il tag, GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che desideri monitorare. 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn :

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	<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>
Gestisci manualmente l'agente di GuardDuty sicurezza	1. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. Assicurati di non abilitare Runtime Monitoring - Configurazione automatica degli agenti per nessuno degli account selezionati. 2. Scegli Conferma. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione dell'agente automatizzato per un account autonomo

A un account autonomo spetta la decisione di abilitare o disabilitare un piano di protezione in uno specifico account Account AWS . Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione del monitoraggio del runtime per ambienti con più account](#).

Dopo aver abilitato il Runtime Monitoring, assicurati GuardDuty di installare Security Agent tramite la configurazione automatica o la distribuzione manuale. Come parte del completamento di tutti i passaggi elencati nella procedura seguente, assicuratevi di installare il security agent.

In base alla tua preferenza di monitorare tutte le risorse Amazon EKS o solo alcune, scegli un metodo preferito e segui i passaggi indicati nella tabella seguente.

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Runtime Monitoring.

3. Nella scheda Configurazione, scegli Abilita per abilitare la configurazione automatica degli agenti per il tuo account.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	1. Scegli Abilita nella sezione Configurazione automatica dell'agente. GuardDuty gestirà l'implementazione e gli aggiornamenti del security agent per tutti i cluster EKS esistenti e potenzialmente nuovi nel tuo account. 2. Scegli Save (Salva).

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave <code>GuardDutyManaged</code> e il valore corrispondente <code>false</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <code>ec2:CreateTags</code> con <code>eks:TagResource</code> . • Sostituisci <code>ec2:DeleteTags</code> con <code>eks:UntagResource</code> . • Sostituisci con <code>access-project</code> GuardDuty Managed • Sostituisci <code>123456789012</code> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-</pre>

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	<pre>admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring.  Note Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, l'agente GuardDuty di sicurezza verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, scegli Abilita nella sezione Gestione degli agenti. GuardDuty Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Scegli Save (Salva). Per escludere un cluster EKS dal monitoraggio dopo che il GuardDuty security agent è già stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave GuardDutyManaged e il valore corrispondente false.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Dopo questo passaggio, non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci con <i>access-project</i> GuardDuty Managed • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:</pre>

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	<code>iam::123456789012:role/org-admins/iam-admin"]</code> 3. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	1. Assicurati di scegliere Disabilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Seleziona Salva 3. Aggiungi un tag a questo cluster EKS con la chiave <code>GuardDutyManaged</code> e il valore corrispondente <code>true</code>. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà l'implementazione e gli aggiornamenti del security agent per i cluster EKS selettivi che desideri monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <code>ec2:CreateTags</code> con <code>eks:TagResource</code> . • Sostituisci <code>ec2:DeleteTags</code> con <code>eks:UntagResource</code> . • Sostituisci con <code>access-project</code> GuardDuty Managed • Sostituisci <code>123456789012</code> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn :

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi <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>
Gestire l'agente manualmente	1. Assicurati di scegliere Disabilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Scegli Save (Salva). 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Questa sezione descrive come gestire il tuo agente aggiuntivo Amazon EKS (GuardDuty agente) dopo aver abilitato Runtime Monitoring (o EKS Runtime Monitoring). Per utilizzare Runtime Monitoring, devi abilitare Runtime Monitoring e configurare il componente aggiuntivo Amazon EKS,aws-guardduty-agent. È necessario eseguire entrambi i passaggi per GuardDuty rilevare e generare [GuardDuty Tipi di risultati del monitoraggio del runtime](#) potenziali minacce.

Per gestire l'agente manualmente, è necessario creare un endpoint VPC come prerequisito. Questo aiuta a GuardDuty ricevere gli eventi di runtime. Successivamente, puoi installare il security agent in modo che inizi GuardDuty a ricevere gli eventi di runtime dalle risorse Amazon EKS. Quando GuardDuty rilascia una nuova versione dell'agente per questa risorsa, puoi aggiornare la versione dell'agente nel tuo account.

Argomenti

- [Prerequisito: creazione di un endpoint Amazon VPC](#)
- [Installazione manuale dell'agente di GuardDuty sicurezza sulle risorse Amazon EKS](#)

- [Aggiornamento manuale dell'agente di sicurezza per le risorse Amazon EKS](#)

Prerequisito: creazione di un endpoint Amazon VPC

Prima di poter installare il GuardDuty security agent, devi creare un endpoint Amazon Virtual Private Cloud (Amazon VPC). Questo ti aiuterà a GuardDuty ricevere gli eventi di runtime delle tue risorse Amazon EKS.

Note

Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint VPC.

Scegli un metodo di accesso preferito per creare un endpoint Amazon VPC.

Console

Per creare un endpoint VPC

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Dal riquadro di navigazione, in Cloud privato virtuale, scegli Endpoint.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nella pagina Crea endpoint per Categoria servizio, scegli Altri servizi endpoint.
5. Per Nome servizio, inserisci **com.amazonaws.us-east-1.guardduty-data**.

Assicurati di sostituirlo **us-east-1** con la regione corretta. Questa deve essere la stessa regione del cluster EKS che appartiene al tuo Account AWS ID.

6. Scegli Verifica del servizio.
7. Dopo aver verificato correttamente il nome del servizio, scegli il VPC in cui risiede il cluster. Aggiungi la policy seguente per limitare l'utilizzo degli endpoint VPC solo all'account specificato. Con la Condition dell'organizzazione fornita sotto a questa policy, puoi aggiornare la policy seguente per limitare l'accesso all'endpoint. Per fornire il supporto degli endpoint VPC a un account IDs specifico della tua organizzazione, consulta. [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 account di `aws:PrincipalAccount` deve corrispondere all'account contenente il VPC e l'endpoint VPC. L'elenco seguente mostra come condividere l'endpoint VPC con altri Account AWS IDs

Condizione dell'organizzazione per limitare l'accesso all'endpoint

- Per specificare più account per accedere all'endpoint VPC, sostituisci `"aws:PrincipalAccount": "111122223333"` con quanto segue:

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
]
```

- Per consentire a tutti i membri di un'organizzazione di accedere all'endpoint VPC, sostituisci "aws:PrincipalAccount": "**111122223333**" con quanto segue:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Per limitare l'accesso a una risorsa da parte di un ID organizzazione, aggiungi il tuo ResourceOrgID alla policy.

[Per ulteriori informazioni, consulta ResourceOrg ID.](#)

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. In Impostazioni aggiuntive, scegli Abilita nome DNS.
9. In Sottoreti, scegli le sottoreti in cui risiede il cluster.
10. In Gruppi di sicurezza, scegli un gruppo di sicurezza con la porta 443 in ingresso abilitata dal tuo VPC (o dal cluster EKS). Se non disponi già di un gruppo di sicurezza con una porta 443 in ingresso abilitata, [Crea un gruppo di sicurezza](#).

Se c'è un problema durante la limitazione delle autorizzazioni in ingresso al tuo VPC (o istanza), puoi utilizzare la porta 443 in ingresso da qualsiasi indirizzo IP. (0.0.0.0/0)
Tuttavia, GuardDuty consiglia di utilizzare indirizzi IP che corrispondano al blocco CIDR per il VPC. Per ulteriori informazioni, consulta i [blocchi VPC CIDR](#) nella Amazon VPC User Guide.

API/CLI

Per creare un endpoint VPC

- Invoca. [CreateVpcEndpoint](#)
- Utilizza i seguenti valori per i parametri:
 - Per Nome servizio, inserisci **com.amazonaws.us-east-1.guardduty-data**.

Assicurati di sostituirlo **us-east-1** con la regione corretta. Questa deve essere la stessa regione del cluster EKS che appartiene al tuo Account AWS ID.

- Per [DNSOptions](#), abilita l'opzione DNS privato impostandola su true.
- Per AWS Command Line Interface, vedi [create-vpc-endpoint](#).

Dopo aver seguito i passaggi, verifica [Convalida della configurazione degli endpoint VPC](#) che l'endpoint VPC sia stato configurato correttamente.

Installazione manuale dell'agente di GuardDuty sicurezza sulle risorse Amazon EKS

Questa sezione descrive come implementare il GuardDuty security agent per la prima volta per cluster EKS specifici. Prima di procedere con questa sezione, assicuratevi di aver già impostato i prerequisiti e abilitato il Runtime Monitoring per i vostri account. Il GuardDuty security agent (componente aggiuntivo EKS) non funzionerà se non abilitate il Runtime Monitoring.

Scegliete il metodo di accesso preferito per implementare il GuardDuty security agent per la prima volta.

Console

1. Apri la console Amazon EKS a <https://console.aws.amazon.com/eks/home#/clusters>.
2. Scegli il Nome cluster.
3. Selezionare la scheda Componenti aggiuntivi.
4. Scegli Ottieni altri componenti aggiuntivi.
5. Nella pagina Seleziona componenti aggiuntivi, scegli Amazon GuardDuty EKS Runtime Monitoring.
6. GuardDuty consiglia di scegliere la versione più recente e predefinita dell'agente.
7. Nella pagina Configura le impostazioni dei componenti aggiuntivi selezionati, utilizza le impostazioni predefinite. Se lo stato del componente aggiuntivo EKS è Richiede attivazione, scegli Attiva GuardDuty. Questa azione aprirà la GuardDuty console per configurare il monitoraggio del runtime per i tuoi account.
8. Dopo aver configurato il Runtime Monitoring per i tuoi account, torna alla console Amazon EKS. Lo Stato del componente aggiuntivo EKS dovrebbe essere stato modificato in Pronto per l'installazione.
9. (Facoltativo) Fornitura dello schema di configurazione aggiuntivo EKS

Per la versione aggiuntiva, se si sceglie la versione 1.5.0 o successiva, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per informazioni sugli intervalli di parametri, vedere. [Configura i parametri aggiuntivi EKS](#)

- a. Espandi le impostazioni di configurazione opzionali per visualizzare i parametri configurabili e il valore e il formato previsti.

- b. Imposta i parametri. I valori devono essere compresi nell'intervallo fornito in [Configura i parametri aggiuntivi EKS](#).
 - c. Scegli Salva modifiche per creare il componente aggiuntivo in base alla configurazione avanzata.
 - d. Per il metodo di risoluzione dei conflitti, l'opzione scelta verrà utilizzata per risolvere un conflitto quando si aggiorna il valore di un parametro a un valore non predefinito. Per ulteriori informazioni sulle opzioni elencate, consulta [ResolveConflicts nell'Amazon EKS API Reference](#).
10. Scegli Next (Successivo).
 11. Nella pagina Rivedi e crea, verifica tutti i dettagli, quindi scegli Crea.
 12. Torna ai dettagli del cluster e scegli la scheda Risorse.
 13. Puoi visualizzare i nuovi pod con il prefisso. `aws-guardduty-agent`

API/CLI

È possibile configurare il componente aggiuntivo di Amazon EKS (`aws-guardduty-agent`) utilizzando una delle opzioni seguenti:

- Corri [CreateAddon](#) per il tuo account.

Note

Per il componente aggiuntivo `version`, se scegli la versione 1.5.0 o successiva, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per ulteriori informazioni, consulta [Configura i parametri aggiuntivi EKS](#).

Utilizza i valori seguenti per i parametri della richiesta:

- In `addonName`, immettere `aws-guardduty-agent`.

È possibile utilizzare il seguente AWS CLI esempio quando si utilizzano valori configurabili supportati per versioni aggiuntive o successive. `v1.5.0` Assicurati di sostituire i valori segnaposto evidenziati in rosso e quelli `Example.json` associati ai valori configurati.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.12.1-eksbuild.2 --configuration-values 'file:///example.json'
```

Example Esempio.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

- Per informazioni sulle `addonVersion` supportate, consulta [Versioni di Kubernetes supportate dal security agent GuardDuty](#).
- In alternativa, puoi usare AWS CLI. Per ulteriori informazioni, consulta [create-addon](#).

Nomi DNS privati per endpoint VPC

Per impostazione predefinita, il security agent si risolve e si connette al nome DNS privato dell'endpoint VPC. Per un endpoint non FIPS, il DNS privato verrà visualizzato nel seguente formato:

Endpoint non FIPS: `guardduty-data.us-east-1.amazonaws.com`

Il Regione AWS, *us-east-1*, cambierà in base alla tua regione.

Aggiornamento manuale dell'agente di sicurezza per le risorse Amazon EKS

Quando gestisci manualmente il GuardDuty security agent, hai la responsabilità di aggiornarlo per il tuo account. Per ricevere notifiche sulle nuove versioni degli agenti, puoi abbonarti a un feed RSS a [GuardDuty versioni di rilascio di Security Agent](#).

È possibile aggiornare il Security Agent alla versione più recente per beneficiare del supporto e dei miglioramenti aggiuntivi. Se la versione corrente dell'agente sta per terminare il supporto standard, per continuare a utilizzare Runtime Monitoring (o EKS Runtime Monitoring), è necessario eseguire l'aggiornamento a una versione dell'agente successiva disponibile o all'ultima versione dell'agente.

Prerequisito

Prima di aggiornare la versione del Security Agent, assicurati che la versione dell'agente che intendi utilizzare ora sia compatibile con la tua versione di Kubernetes. Per ulteriori informazioni, consulta [Versioni di Kubernetes supportate dal security agent GuardDuty](#).

Console

1. Apri la console Amazon EKS a <https://console.aws.amazon.com/eks/home#/clusters>.
2. Scegli il Nome cluster.
3. Nella sezione Informazioni sul cluster, scegli la scheda Componenti aggiuntivi.
4. Nella scheda Componenti aggiuntivi, seleziona GuardDutyEKS Runtime Monitoring.
5. Scegli Modifica per aggiornare i dettagli dell'agente.
6. Nella pagina Configure GuardDuty EKS Runtime Monitoring, aggiorna i dettagli.
7. (Facoltativo) Aggiornamento delle impostazioni di configurazione opzionali

Se la versione del componente aggiuntivo EKS è 1.5.0 o superiore, puoi anche aggiornare lo schema di configurazione del componente aggiuntivo.

- a. Espandi Impostazioni di configurazione opzionali per visualizzare lo schema di configurazione.
- b. Aggiorna i valori dei parametri in base all'intervallo fornito in [Configura i parametri aggiuntivi EKS](#).
- c. Scegli Salva modifiche per avviare l'aggiornamento.
- d. Per il metodo di risoluzione dei conflitti, l'opzione scelta verrà utilizzata per risolvere un conflitto quando si aggiorna il valore di un parametro a un valore non predefinito. Per

ulteriori informazioni sulle opzioni elencate, consulta [ResolveConflicts nell'Amazon EKS API Reference](#).

API/CLI

Per aggiornare l'agente GuardDuty di sicurezza per i tuoi cluster Amazon EKS, consulta [Aggiornamento di un componente aggiuntivo](#).

Note

Per il componente aggiuntivo `version`, se scegli la versione 1.5.0 o una versione successiva, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per informazioni sugli intervalli di parametri, vedere. [Configura i parametri aggiuntivi EKS](#)

È possibile utilizzare l' AWS CLI esempio seguente quando si utilizzano valori configurabili supportati per le versioni aggiuntive 1.5.0 e successive. Assicurati di sostituire i valori segnaposto evidenziati in rosso e quelli associati ai `Example.json` valori configurati.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.12.1-eksbuild.2 --configuration-values 'file://example.json'
```

Example Esempio.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

Se la tua versione del componente aggiuntivo Amazon EKS è 1.5.0 o successiva e hai configurato lo schema del componente aggiuntivo, puoi verificare se i valori vengono visualizzati correttamente per il tuo cluster. Per ulteriori informazioni, consulta [Verifica degli aggiornamenti dello schema di configurazione](#).

Configurazione GuardDuty dei parametri dell'agente di sicurezza (componente aggiuntivo) per Amazon EKS

Puoi configurare parametri specifici del tuo agente di GuardDuty sicurezza per Amazon EKS. Questo supporto è disponibile per la versione 1.5.0 e successive del GuardDuty Security Agent. Per informazioni sulle ultime versioni dei componenti aggiuntivi, consulta. [GuardDuty versioni degli agenti di sicurezza per le risorse Amazon EKS](#)

Perché devo aggiornare lo schema di configurazione del Security Agent

Lo schema di configurazione per l'agente GuardDuty di sicurezza è lo stesso per tutti i contenitori all'interno dei cluster Amazon EKS. Quando i valori predefiniti non sono in linea con i carichi di lavoro associati e le dimensioni dell'istanza, prendi in considerazione la configurazione delle impostazioni della CPU, delle impostazioni della memoria e delle impostazioni. `PriorityClass` `dnsPolicy` Indipendentemente da come gestisci l' GuardDuty agente per i tuoi cluster Amazon EKS, puoi configurare o aggiornare la configurazione esistente di questi parametri.

Comportamento di configurazione automatizzato degli agenti con parametri configurati

Quando GuardDuty gestisce il Security Agent (componente aggiuntivo EKS) per conto dell'utente, aggiorna il componente aggiuntivo, se necessario. GuardDuty imposterà il valore dei parametri configurabili su un valore predefinito. Tuttavia, è ancora possibile aggiornare i parametri al valore desiderato. Se ciò causa un conflitto, l'opzione predefinita per [ResolveConflicts](#) è. None

Parametri e valori configurabili

Per informazioni sui passaggi per configurare i parametri del componente aggiuntivo, consulta:

- [Installazione manuale dell'agente di GuardDuty sicurezza sulle risorse Amazon EKS](#) o
- [Aggiornamento manuale dell'agente di sicurezza per le risorse Amazon EKS](#)

Le tabelle seguenti forniscono gli intervalli e i valori che puoi utilizzare per distribuire manualmente il componente aggiuntivo Amazon EKS o aggiornare le impostazioni del componente aggiuntivo esistenti.

Impostazioni della CPU

Parameters	Valore predefinito	Intervallo configurabile
Richieste	200 m	Tra 200 m e 10000 m, entrambi inclusi
Limits	1000 m	

Impostazioni della memoria

Parameters	Valore predefinito	Intervallo configurabile
Richieste	256 Mi	Tra 256 Mi e 20000 Mi, entrambi inclusi
Limits	1024 Mi	

Impostazioni di **PriorityClass**

Quando GuardDuty crea un componente aggiuntivo Amazon EKS per te, l'assegnato **PriorityClass** è `aws-guardduty-agent.priorityclass`. Ciò significa che non verrà intrapresa alcuna azione in base alla priorità del pod dell'agente. È possibile configurare questo parametro aggiuntivo scegliendo una delle seguenti **PriorityClass** opzioni:

Configurabile PriorityClass	preemptionPolicy value	preemptionPolicy descrizione	valore del pod
<code>aws-guardduty-agent.priorityclass</code>	Never	Nessuna operazione	1000000
<code>aws-guardduty-agent.priorityclass-high</code>	PreemptLowerPriority	L'assegnazione di questo valore impedirà l'esecuzione di un pod con il valore di	100000000

Configurabile PriorityClass	preemptionPolicy value	preemptionPolicy descrizione	valore del pod
system-cluster-critical ¹	PreemptLowerPriority	priorità inferiore al valore del pod dell'agente.	2000000000
system-node-critical ¹	PreemptLowerPriority		2000001000

¹ Kubernetes offre queste due opzioni: e. `PriorityClass system-cluster-critical` `system-node-critical` Per ulteriori informazioni, consulta la documentazione di [PriorityClass](#) Kubernetes.

Impostazioni di **dnsPolicy**

Scegli una delle seguenti opzioni di policy DNS supportate da Kubernetes. Quando non viene specificata alcuna configurazione, `ClusterFirst` viene utilizzato come valore predefinito.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Per informazioni su queste politiche, consulta la [politica DNS di Pod nella documentazione](#) di Kubernetes.

Verifica degli aggiornamenti dello schema di configurazione

Dopo aver configurato i parametri, effettuate le seguenti operazioni per verificare che lo schema di configurazione sia stato aggiornato:

1. Apri la console Amazon EKS a <https://console.aws.amazon.com/eks/home#/clusters>.
2. Nel pannello di navigazione scegliere Cluster.
3. Nella pagina Cluster, seleziona il nome del cluster per il quale desideri verificare gli aggiornamenti.

4. Scegli la scheda Risorse.
5. Dal riquadro Tipi di risorse, in Carichi di lavoro, scegli. DaemonSets
6. Seleziona aws-guardduty-agent.
7. Nella aws-guardduty-agent pagina, scegli Visualizzazione raw per visualizzare la risposta JSON non formattata. Verifica che i parametri configurabili visualizzino il valore che hai fornito.

Dopo la verifica, passa alla GuardDuty console. Seleziona il corrispondente Regione AWS e visualizza lo stato della copertura per i tuoi cluster Amazon EKS. Per ulteriori informazioni, consulta [Copertura del runtime e risoluzione dei problemi per i cluster Amazon EKS](#).

Convalida della configurazione degli endpoint VPC

Dopo aver installato il security agent manualmente o tramite la configurazione GuardDuty automatica, puoi utilizzare questo documento per convalidare la configurazione dell'endpoint VPC. Puoi utilizzare questi passaggi anche dopo aver risolto qualsiasi [problema di copertura del runtime](#) per un tipo di risorsa. Puoi assicurarti che i passaggi abbiano funzionato come previsto e che lo stato della copertura venga potenzialmente visualizzato come Integro.

Utilizza i seguenti passaggi per verificare che la configurazione dell'endpoint VPC per il tuo tipo di risorsa sia configurata correttamente nell'account del proprietario del VPC:

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. <https://console.aws.amazon.com/vpc/>
2. Nel pannello di navigazione, in Virtual private cloud, scegli Your VPCs.
3. Nella VPCs pagina I tuoi, scegli IPv4 CIDR associato al tuo ID VPC.
4. Dal riquadro di navigazione, in Cloud privato virtuale, scegli Endpoint.
5. Nella tabella Endpoints, seleziona la riga con il nome del servizio simile a com.amazonaws. **us-east-1**.guardduty-data. La regione (us-east-1) potrebbe essere diversa per il tuo endpoint.
6. Verrà visualizzato un pannello con i dettagli dell'endpoint. Nella scheda Gruppi di sicurezza, seleziona il link ID del gruppo associato per maggiori dettagli.
7. Nella tabella Gruppi di sicurezza, seleziona la riga con l'ID del gruppo di sicurezza associato per visualizzare i dettagli.
8. Nella scheda Regole in entrata, assicurati che esista una politica di ingresso con l'intervallo di porte pari a 443 e Source come valore copiato dal CIDR. IPv4 Le regole in entrata controllano il

traffico in entrata a cui è consentito raggiungere l'istanza. L'immagine seguente mostra le regole in entrata per un gruppo di sicurezza associato al VPC utilizzato GuardDuty dal security agent.

Se non disponi già di un gruppo di sicurezza con una porta in ingresso 443 abilitata, [crea un gruppo di sicurezza](#) nella Amazon EC2 User Guide.

Se c'è un problema durante la limitazione delle autorizzazioni in ingresso al tuo VPC (o cluster), fornisci il supporto alla porta 443 in ingresso da qualsiasi indirizzo IP (0.0.0.0/0).

L'elenco seguente include elementi utili dopo l'installazione o l'aggiornamento del Security Agent.

Valuta la copertura del runtime

Il passaggio successivo dopo l'installazione o l'aggiornamento del security agent consiste nel valutare la copertura in fase di esecuzione delle risorse. Se lo stato di copertura del runtime è Inadeguato, è necessario risolvere il problema. Per ulteriori informazioni, consulta [Problemi di copertura del runtime e risoluzione dei problemi](#).

Se lo stato della copertura in fase di esecuzione risulta integro, significa che Runtime Monitoring è in grado di raccogliere e ricevere eventi di runtime. Per un elenco di questi eventi, vedere [Tipi di eventi di runtime raccolti](#).

Nome DNS privato per l'endpoint

Dopo aver installato il GuardDuty security agent per le tue risorse, per impostazione predefinita, si risolverà e si conatterà al nome DNS privato dell'endpoint VPC. Per un endpoint non FIPS, il DNS privato verrà visualizzato nel seguente formato:

```
guardduty-data.us-east-1.amazonaws.com
```

Il Regione AWS, *us-east-1*, cambierà in base alla tua regione.

Un host può essere installato con due agenti di sicurezza

Quando lavori con un agente GuardDuty di sicurezza per un'istanza Amazon EC2, puoi installare e utilizzare l'agente sull'host sottostante all'interno di un cluster Amazon EKS. Se hai già implementato un agente di sicurezza su quel cluster EKS, sullo stesso host potrebbero essere in esecuzione due agenti di sicurezza contemporaneamente. Per informazioni su come GuardDuty funziona in questo scenario, consulta [Agenti di sicurezza sullo stesso host](#).

Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi

Dopo aver abilitato il Runtime Monitoring e aver installato il GuardDuty security agent sulla risorsa, GuardDuty fornisce le statistiche di copertura per il tipo di risorsa corrispondente e lo stato di copertura individuale per le risorse che appartengono al tuo account. Lo stato della copertura viene determinato assicurandoti di aver abilitato il Runtime Monitoring, che l'endpoint Amazon VPC sia stato creato e che sia stato GuardDuty distribuito il security agent per la risorsa corrispondente. Uno stato di copertura integro indica che, quando si verifica un evento di runtime relativo alla risorsa, GuardDuty è in grado di ricevere tale evento di runtime tramite l'endpoint Amazon VPC e monitorarne il comportamento. Se si è verificato un problema al momento della configurazione del Runtime Monitoring, della creazione di un endpoint Amazon VPC o GuardDuty della distribuzione del security agent, lo stato di copertura appare come Non integro. Quando lo stato di copertura non è integro, non GuardDuty sarà in grado di ricevere o monitorare il comportamento di runtime della risorsa corrispondente o generare alcun risultato di Runtime Monitoring.

I seguenti argomenti ti aiuteranno a rivedere le statistiche sulla copertura, configurare EventBridge le notifiche e risolvere i problemi di copertura per un tipo di risorsa specifico.

Indice

- [Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2](#)
- [Copertura del runtime e risoluzione dei problemi per i cluster Amazon ECS](#)
- [Copertura del runtime e risoluzione dei problemi per i cluster Amazon EKS](#)

Copertura del runtime e risoluzione dei problemi per l'istanza Amazon EC2

Per una risorsa Amazon EC2, la copertura del runtime viene valutata a livello di istanza. Le tue istanze Amazon EC2 possono eseguire diversi tipi di applicazioni e carichi di lavoro, tra gli altri, nel tuo ambiente. AWS Questa funzionalità supporta anche le istanze Amazon EC2 gestite da Amazon ECS e se hai cluster Amazon ECS in esecuzione su un'istanza Amazon EC2, i problemi di copertura a livello di istanza verranno visualizzati nella copertura del runtime di Amazon EC2.

Argomenti

- [Revisione delle statistiche di copertura](#)
- [Modifica dello stato della copertura con notifiche EventBridge](#)

- [Risoluzione dei problemi di copertura del runtime di Amazon EC2](#)

Revisione delle statistiche di copertura

Le statistiche di copertura per le istanze Amazon EC2 associate ai tuoi account o ai tuoi account membro sono la percentuale delle istanze EC2 integre rispetto a tutte le istanze EC2 selezionate. Regione AWS L'equazione seguente rappresenta questa percentuale come:

$$(\text{Istanze sane}) * 100 / \text{instances/All}$$

Se hai anche distribuito l'agente di GuardDuty sicurezza per i tuoi cluster Amazon ECS, qualsiasi problema di copertura a livello di istanza associato ai cluster Amazon ECS in esecuzione su un'istanza Amazon EC2 verrà visualizzato come un problema di copertura del runtime dell'istanza Amazon EC2.

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi a e apri la console all'indirizzo. Console di gestione AWS GuardDuty <https://console.aws.amazon.com/guardduty/>
- Nel riquadro di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Runtime coverage.
- Nella scheda Copertura del runtime dell'istanza EC2, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura di ogni istanza Amazon EC2 disponibile nella tabella Elenco istanze.
 - Puoi filtrare la tabella dell'elenco delle istanze in base alle seguenti colonne:
 - ID account
 - Tipo di gestione dell'agente
 - Versione dell'agente
 - Stato copertura
 - ID dell'istanza
 - ARN del cluster
 - Se una delle tue istanze EC2 ha lo stato di copertura come Non integro, la colonna Problema include informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Esegui l'[ListCoverage](#) API con il tuo ID rilevatore, la tua regione corrente e l'endpoint di servizio validi. Puoi filtrare e ordinare l'elenco delle istanze utilizzando questa API.
- Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
 - `ACCOUNT_ID`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `AGENT_VERSION`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
 - `CLUSTER_ARN`
- Quando `filter-criteria` include `RESOURCE_TYPE EC2`, Runtime Monitoring non supporta l'uso di `ISSUE` come `AttributeName`. Se lo usi, la risposta dell'API risulterà `InvalidInputException`.

Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:

- `ACCOUNT_ID`
- `COVERAGE_STATUS`
- `INSTANCE_ID`
- `UPDATED_AT`
- È possibile modificare *`max-results`* (fino a 50).
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui 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
```

- Esegui l'[GetCoverageStatistics](#) API per recuperare le statistiche aggregate sulla copertura basate su. `statisticsType`
- Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:
 - `COUNT_BY_COVERAGE_STATUS`: rappresenta le statistiche di copertura per i cluster EKS aggregate per stato di copertura.
 - `COUNT_BY_RESOURCE_TYPE`— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
- È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
 - `ACCOUNT_ID`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `AGENT_VERSION`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
 - `CLUSTER_ARN`
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui 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"}}] }'
```

Se lo stato di copertura della tua istanza EC2 è Inadeguato, consulta. [Risoluzione dei problemi di copertura del runtime di Amazon EC2](#)

Modifica dello stato della copertura con notifiche EventBridge

Lo stato di copertura dell'istanza Amazon EC2 potrebbe apparire come Non integro. Per sapere quando lo stato della copertura cambia, ti consigliamo di monitorare periodicamente lo stato della copertura e di risolvere i problemi se lo stato diventa Non integro. In alternativa, puoi creare una [EventBridge](#) regola Amazon per ricevere una notifica quando lo stato della copertura cambia da

Insalutare a Healthy o altro. Per impostazione predefinita, GuardDuty lo pubblica nel [EventBridge bus](#) relativo al tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta [Create rule](#) nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura della tua istanza Amazon EC2 cambia da Healthy aUnhealthy, detail-type dovresti farlo. *GuardDuty Runtime Protection Unhealthy* Per ricevere una notifica quando lo stato della copertura cambia da Unhealthy aHealthy, sostituisci il valore di detail-type con*GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione 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"
  }
}

```

Risoluzione dei problemi di copertura del runtime di Amazon EC2

Se lo stato di copertura della tua istanza Amazon EC2 non è integro, puoi visualizzare il motivo nella colonna Problema.

Se la tua istanza EC2 è associata a un cluster EKS e l'agente di sicurezza per EKS è stato installato manualmente o tramite una configurazione automatica dell'agente, per risolvere il problema di copertura, consulta. [Copertura del runtime e risoluzione dei problemi per i cluster Amazon EKS](#)

La tabella seguente elenca i tipi di problemi e le relative procedure di risoluzione.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Nessuna segnalazione da parte dell'agente	In attesa di una notifica via SMS	La ricezione della notifica SSM potrebbe richiedere alcuni minuti. Assicurati che l'istanza Amazon EC2 sia gestita tramite SSM. Per ulteriori informazioni, vedere la procedura riportata in Metodo 1 - Usare AWS Systems Manager in Installazione manuale del security agent .
	(Vuoto apposta)	Se gestisci il GuardDuty Security Agent manualmente, assicurati di aver seguito i passaggi seguenti Gestione manuale dell'agente di

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
		sicurezza per la risorsa Amazon EC2. Se hai abilitato la configurazione automatica dell'agente: • La tua istanza EC2 è gestita tramite SSM. • Visualizza periodicamente lo stato del tuo agente di sicurezza. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent. Verifica che l'endpoint VPC per la tua istanza Amazon EC2 sia configurato correttamente. Per ulteriori informazioni, consulta Convalida della configurazione degli endpoint VPC.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
		Se la tua organizzazione ha una policy di controllo dei servizi (SCP), verifica che il limite delle autorizzazioni non limiti l'autorizzazione. <code>guardduty:SendSecurityTelemetry</code> Per ulteriori informazioni, consulta Convalida della politica di controllo dei servizi della tua organizzazione in un ambiente con più account.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
	Agente disconnesso	• Visualizza lo stato del tuo agente di sicurezza. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent. • Visualizza i log del Security Agent per identificare la potenziale causa principale. I log forniscono errori dettagliati che è possibile utilizzare per risolvere autonomamente il problema. I file di registro sono disponibili in: <code>/var/log/amzn-guardduty-agent/</code> <pre>Faresudo journalctl -u amazon-guardduty-agent .</pre>
Agente non fornito	Le istanze con tag di esclusione sono escluse dal Runtime Monitoring.	GuardDuty non riceve eventi di runtime dalle istanze Amazon EC2 lanciate con il tag di esclusione: <code>GuardDutyManaged false</code> Per ricevere eventi di runtime da questa istanza Amazon EC2, rimuovi il tag di esclusione.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
	La versione del kernel è inferiore alla versione supportata.	Per informazioni sulle versioni del kernel supportate nelle distribuzioni del sistema operativo, consulta Convalida i requisiti architetturici per le istanze Amazon EC2.
	La versione del kernel è superiore alla versione supportata.	Per informazioni sulle versioni del kernel supportate nelle distribuzioni del sistema operativo, consulta Convalida i requisiti architetturici per le istanze Amazon EC2.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
	Impossibile recuperare il documento di identità dell'istanza.	Completare la procedura riportata di seguito. 1. Verifica che la tua risorsa sia un'istanza Amazon EC2 e non un'istanza ibrida non EC2. 2. Verifica che l'Instance Metadata Service (IMDS) sia abilitato. A tale scopo, consulta Configure Instance Metadata Service options nella Amazon EC2 User Guide. 3. Verifica che il documento di identità dell'istanza esista. A tale scopo, consulta Recupera il documento di identità dell'istanza nella Guida per l'utente di Amazon EC2. 4. Se il documento di identità dell'istanza non esiste ancora, riavvia l'istanza. Il documento di identità dell'istanza viene generato quando l'istanza viene arrestata e avviata, riavviata o avviata.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Creazione dell'associazione SSM non riuscita	GuardDuty L'associazione SSM esiste già nel tuo account	1. Elimina manualmente l'associazione esistente. Per ulteriori informazioni, vedere Eliminazione delle associazioni nella Guida per l'AWS Systems Manager utente. 2. Dopo aver eliminato l'associazione, disabilita e riattiva la configurazione GuardDuty automatica dell'agente per Amazon EC2.
	Il tuo account ha troppe associazioni SSM	Scegli una delle due opzioni seguenti: • Eliminare tutte le associazioni SSM non utilizzate. Per ulteriori informazioni, consulta Eliminazione delle associazioni nella Guida per l'AWS Systems Manager utente. • Verifica se il tuo account è idoneo per un aumento della quota. Per ulteriori informazioni, vedere le quote del servizio Systems Manager nel Riferimenti generali di AWS.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Aggiornamento dell'associazione SSM non riuscito	GuardDuty L'associazione SSM non esiste nel tuo account	GuardDuty L'associazione SSM non è presente nel tuo account. Disabilita e riattiva il monitoraggio del runtime.
Eliminazione dell'associazione SSM non riuscita	GuardDuty L'associazione SSM non esiste nel tuo account	L'associazione SSM non è presente nel tuo account. Se l'associazione SSM è stata eliminata intenzionalmente, non è necessaria alcuna azione.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Esecuzione dell'associazione di istanze SSM non riuscita	I requisiti architetturici o altri prerequisiti non sono soddisfatti.	Per informazioni sulle distribuzioni verificate del sistema operativo, vedere. Prerequisiti per il supporto delle istanze Amazon EC2 Se il problema persiste, i seguenti passaggi ti aiuteranno a identificare e potenzialmente risolvere il problema: 1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/. 2. Nel riquadro di navigazione, in Gestione dei nodi, seleziona State Manager. 3. Filtra per proprietà Document Name e inserisci AmazonGuardDuty-ConfigureRuntimeMonitoringSsm Plugin. 4. Seleziona l'ID dell'associazione corrispondente e visualizzatene la cronologia di esecuzione. 5. Utilizzando la cronologia di esecuzione, visualizza gli errori, identifica la

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
		potenziale causa principale e prova a risolverla.
Creazione degli endpoint VPC non riuscita	La creazione di endpoint VPC non è supportata per VPC condiviso <i>vpcId</i>	Il Runtime Monitoring supporta l'uso di un VPC condiviso all'interno di un'organizzazione. Per ulteriori informazioni, consulta Utilizzo di un VPC condiviso con Runtime Monitoring .
	Solo quando si utilizza un VPC condiviso con configurazione automatica degli agenti L'ID dell'account proprietario <i>111122223333</i> per il VPC condiviso <i>vpcId</i> non ha né il monitoraggio del runtime né la configurazione automatica degli agenti abilitati o entrambi	L'account proprietario del VPC condiviso deve abilitare il monitoraggio del runtime e la configurazione automatica degli agenti per almeno un tipo di risorsa (Amazon EKS o Amazon ECS (Fargate)). Per ulteriori informazioni, consulta Prerequisiti specifici per il monitoraggio del runtime GuardDuty .

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
	L'abilitazione del DNS privato richiede entrambi <code>enableDnsSupport</code> e gli attributi <code>enableDnsHostnames</code> VPC impostati <code>true</code> su <i>vpcId</i> for (Service: Ec2, Status Code:400, Request ID:). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>	Assicurati che i seguenti attributi VPC siano impostati su <code>true</code> – <code>enableDnsSupport</code> e <code>enableDnsHostnames</code> . Per ulteriori informazioni, consulta Attributi DNS nel VPC. Se utilizzi la console Amazon VPC su https://console.aws.amazon.com/vpc/ per creare Amazon VPC, seleziona sia <code>Abilita nomi host DNS</code> che <code>Abilita risoluzione DNS</code>. Per ulteriori informazioni, consulta Opzioni di configurazione del VPC. Dopo aver aggiornato gli attributi VPC, devi accelerare un nuovo tentativo di creazione dell'endpoint VPC apportando una delle seguenti modifiche: • Puoi aggiungere o modificare il <code>GuardDutyManaged</code> tag per la tua istanza Amazon EC2 (consigliato). Ad esempio, puoi aggiungere <code>eGuardDutyManaged</code> : <code>true</code> per includere l'istanza per Runtime Monitoring.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
		Puoi modificare lo stato dell'istanza Amazon EC2 (arresto o riavvio).
Eliminazione degli endpoint VPC condivisi non riuscita	L'eliminazione dell'endpoint VPC condiviso non è consentita per ID account, VPC 111122223333 vpcId condiviso, ID account proprietario. 555555555555	Potenziali passaggi: - La disabilitazione dello stato di monitoraggio del runtime dell'account partecipante VPC condiviso non influisce sulla policy degli endpoint VPC condivisi e sul gruppo di sicurezza esistente nell'account del proprietario. Per eliminare l'endpoint VPC condiviso e il gruppo di sicurezza, devi disabilitare il monitoraggio del runtime o lo stato di configurazione automatica dell'agente nell'account proprietario del VPC condiviso. - L'account partecipante VPC condiviso non può eliminare l'endpoint VPC condiviso e il gruppo di sicurezza ospitati nell'account proprietario del VPC condiviso.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
L'agente non effettua la segnalazione	(Vuoto apposta)	Il tipo di problema ha raggiunto la fine del supporto. Se continui a riscontrare questo problema e non lo hai ancora fatto, abilita l'agente GuardDuty automatizzato per Amazon EC2. Se il problema persiste, prendi in considerazione la possibilità di disattivare il Runtime Monitoring per alcuni minuti, quindi riattivalo.

Copertura del runtime e risoluzione dei problemi per i cluster Amazon ECS

La copertura del runtime per i cluster Amazon ECS include le attività in esecuzione e le istanze di AWS Fargate container Amazon ECS. ¹

Per un cluster Amazon ECS eseguito su Fargate, la copertura del runtime viene valutata a livello di attività. La copertura del runtime dei cluster ECS include le attività Fargate che sono iniziate a essere eseguite dopo aver abilitato il monitoraggio del runtime e la configurazione automatica degli agenti per Fargate (solo ECS). Per impostazione predefinita, un'attività Fargate è immutabile. GuardDuty non sarà in grado di installare il security agent per monitorare i contenitori sulle attività già in esecuzione. Per includere un'attività Fargate di questo tipo, è necessario interromperla e riavviarla. Assicurati di controllare se il servizio associato è supportato.

Per informazioni sul contenitore Amazon ECS, consulta [Creazione di capacità](#).

Indice

- [Revisione delle statistiche di copertura](#)
- [Modifica dello stato della copertura con EventBridge notifiche](#)
- [Risoluzione dei problemi di copertura del runtime di Amazon ECS-Fargate](#)

Revisione delle statistiche di copertura

Le statistiche di copertura per le risorse Amazon ECS associate al tuo account o ai tuoi account membro sono la percentuale di cluster Amazon ECS integri rispetto a tutti i cluster Amazon ECS selezionati. Regione AWS Ciò include la copertura per i cluster Amazon ECS associati alle istanze Fargate e Amazon EC2. L'equazione seguente rappresenta questa percentuale come:

$$(\text{Cluster sani}) * 100 / \text{clusters/All}$$

Considerazioni

- Le statistiche di copertura per il cluster ECS includono lo stato di copertura delle attività Fargate o delle istanze di container ECS associate a quel cluster ECS. Lo stato di copertura delle attività di Fargate include le attività che sono in esecuzione o che sono state completate di recente.
- Nella scheda Copertura del runtime dei cluster ECS, il campo Istanze di container coperte indica lo stato di copertura delle istanze di container associate al tuo cluster Amazon ECS.

Se il tuo cluster Amazon ECS contiene solo attività Fargate, il conteggio appare come 0/0.

- Se il tuo cluster Amazon ECS è associato a un'istanza Amazon EC2 che non dispone di un agente di sicurezza, anche il cluster Amazon ECS avrà uno stato di copertura non salutare.

Per identificare e risolvere il problema di copertura per l'istanza Amazon EC2 associata, consulta per le istanze [Risoluzione dei problemi di copertura del runtime di Amazon EC2](#) Amazon EC2.

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi a Console di gestione AWS e apri la console all'indirizzo. GuardDuty <https://console.aws.amazon.com/guardduty/>
- Nel riquadro di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Runtime coverage.
- Nella scheda Runtime Coverage dei cluster ECS, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura di ogni cluster Amazon ECS disponibile nella tabella Elenco dei cluster.
 - Puoi filtrare la tabella dell'elenco dei cluster in base alle seguenti colonne:
 - ID account

- Nome del cluster
- Tipo di gestione dell'agente
- Stato copertura
- Se uno dei tuoi cluster Amazon ECS ha lo stato di copertura come Non integro, la colonna Problema include informazioni aggiuntive sul motivo dello stato Non integro.

Se i tuoi cluster Amazon ECS sono associati a un'istanza Amazon EC2, vai alla scheda di copertura del runtime dell'istanza EC2 e filtra in base al campo Nome cluster per visualizzare il problema associato.

API/CLI

- Esegui l'[ListCoverage](#) API con il tuo ID di rilevamento, la tua regione corrente e l'endpoint di servizio validi. Puoi filtrare e ordinare l'elenco delle istanze utilizzando questa API.
- Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`
- Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:
 - `ACCOUNT_ID`
 - `COVERAGE_STATUS`
 - `ISSUE`
 - `ECS_CLUSTER_NAME`
 - `UPDATED_AT`

Il campo viene aggiornato solo quando viene creata una nuova attività nel cluster Amazon ECS associato o quando viene modificato lo stato di copertura corrispondente.

- È possibile modificare *max-results* (fino a 50).
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o


```
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
```

- Esegui l'[GetCoverageStatistics](#) API per recuperare le statistiche aggregate sulla copertura basate su `statisticsType`
- Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:
 - `COUNT_BY_COVERAGE_STATUS`— Rappresenta le statistiche di copertura per i cluster ECS aggregate per stato di copertura.
 - `COUNT_BY_RESOURCE_TYPE`— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
 - È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui 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"}}] }'
```

Per ulteriori informazioni sui problemi di copertura, consulta [Risoluzione dei problemi di copertura del runtime di Amazon ECS-Fargate](#).

Modifica dello stato della copertura con EventBridge notifiche

Lo stato di copertura del tuo cluster Amazon ECS potrebbe apparire come Non integro. Per sapere quando lo stato della copertura cambia, ti consigliamo di monitorare periodicamente lo stato della copertura e di risolvere i problemi se lo stato diventa Non integro. In alternativa, puoi creare una EventBridge regola Amazon per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy o altro. Per impostazione predefinita, GuardDuty lo pubblica nel [EventBridge bus](#) relativo al tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta [Create rule](#) nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura del tuo cluster Amazon ECS cambia da Healthy aUnhealthy, detail-type dovresti farlo. *GuardDuty Runtime Protection Unhealthy* Per ricevere una notifica quando lo stato della copertura cambia da Unhealthy aHealthy, sostituisci il valore di detail-type con*GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione 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"
}
}

```

Risoluzione dei problemi di copertura del runtime di Amazon ECS-Fargate

Se lo stato di copertura del tuo cluster Amazon ECS non è integro, puoi visualizzare il motivo nella colonna Problema.

La tabella seguente fornisce i passaggi consigliati per la risoluzione dei problemi di Fargate (solo Amazon ECS). Per informazioni sui problemi di copertura delle istanze Amazon EC2, consulta [Risoluzione dei problemi di copertura del runtime di Amazon EC2](#) per le istanze Amazon EC2.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
L'agente non effettua la segnalazione	Agente che non effettua la segnalazione delle attività in TaskDefinition - 'TASK_DEFINITION'	Verifica che l'endpoint VPC per l'attività del tuo cluster Amazon ECS sia configurato correttamente. Per ulteriori informazioni, consulta Convalida della configurazione degli endpoint VPC. Se la tua organizzazione ha una policy di controllo dei servizi (SCP), verifica che il limite delle autorizzazioni non limiti l'autorizzazione. <code>guardduty:SendSecu</code>

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
L'agente è uscito		rityTelemetry Per ulteriori informazioni, consulta Convalida della politica di controllo dei servizi dell'organizzazione in un ambiente con più account.
	<i>VPC_ISSUE</i> ; for task in TaskDefinition - <i>'TASK_DEFINITION'</i>	Visualizza i dettagli del problema del VPC nelle informazioni aggiuntive.
	ExitCode: EXIT_CODE per le attività in TaskDefinition - <i>'TASK_DEFINITION'</i>	Visualizza i dettagli del problema nelle informazioni aggiuntive.
	Motivo: <i>REASON</i> per attività in TaskDefinition - <i>'TASK_DEFINITION'</i> ExitCode: EXIT_CODE con motivo: <i>'EXIT_CODE'</i> per le attività in TaskDefinition - <i>'TASK_DEFINITION'</i>	

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	Agente chiuso: Motivo:CannotPullContainerError : pull image manifest è stato riprovato...	In questo scenario, non GuardDuty è potenzialmente in grado di recuperare e l'immagine del contenitore del sidecar. L'attività continuerà a funzionare ma non sarà GuardDuty possibile rilevare potenziali minacce. Esegui i seguenti passaggi di risoluzione dei problemi uno alla volta per verificare se aiuta a risolvere il problema di copertura: • Autorizzazioni: assicurati che il tuo ruolo di esecuzione e delle attività disponga delle autorizzazioni ECR richieste elencate in. Requisiti per le autorizzazioni • Connettività di rete: verifica che le attività di Fargate possano raggiungere l'ECR tramite l'accesso pubblico a Internet o gli endpoint VPC configurati correttamente, come descritto in. Requisiti di connessione di rete • Configurazione del gruppo di sicurezza: verifica che il gruppo di sicurezza consenta l'accesso in uscita

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		all'elenco dei prefissi gestiti di S3 sulla porta 443, come spiegato in. Configurazione del gruppo di sicurezza • Esegui il AWS Support TroubleshootECSTaskFailedToStart runbook nella regione del cluster per identificare problemi specifici. • Visualizza i registri delle attività per i messaggi di errore. Per informazioni su come eseguire questa operazione, consulta Visualizzazione dei log degli agenti container di Amazon ECS nella Amazon Elastic Container Service Developer Guide. Per errori comuni e risoluzione dei problemi, consulta la sezione Risoluzione dei problemi di Amazon ECS nella Amazon Elastic Container Service Developer Guide. Questi tre componenti (autorizzazioni, connettività di rete e configurazione del gruppo di sicurezza) sono

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		indipendenti ma tutti necessari per scaricare correttamente l'immagine del GuardDuty contenitore da Amazon ECR. Se il problema persiste, consulta Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto
Creazione degli endpoint VPC non riuscita	L'abilitazione del DNS privato richiede entrambi <code>enableDnsSupport</code> e gli attributi <code>enableDnsHostnames</code> VPC impostati <code>true</code> su <i>vpcId</i> for (Service: EC2, Status Code:400, Request ID:). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>	Assicurati che i seguenti attributi VPC siano impostati su <code>true</code> – <code>enableDnsSupport</code> e <code>enableDnsHostnames</code> . Per ulteriori informazioni, consulta Attributi DNS nel VPC. Se utilizzi la console Amazon VPC su https://console.aws.amazon.com/vpc/ per creare Amazon VPC, assicurati di selezionare sia <code>Abilita nomi host DNS</code> che <code>Abilita risoluzione DNS</code>. Per ulteriori informazioni, consulta Opzioni di configurazione del VPC.
Agente non fornito	Richiamata non supportata da <i>SERVICE</i> for task (s) in TaskDefinition - <i>'TASK_DEFINITION'</i>	Questa attività è stata richiamata da un comando <i>SERVICE</i> non supportato.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	Architettura CPU ' TYPE ' non supportata per le attività in TaskDefinition - ' TASK_DEFINITION '	Questa attività è in esecuzione su un'architettura CPU non supportata. Per informazioni sulle architetture CPU supportate, vedere. Convalida dei requisiti relativi all'architettura
	TaskExecutionRole mancante da TaskDefinition - ' TASK_DEFINITION '	Manca il ruolo di esecuzione e delle attività ECS. Per informazioni su come fornire il ruolo di esecuzione dell'attività e le autorizzazioni richieste, vedere. Prerequisiti per l'accesso all'immagine del contenitore

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	Configurazione di rete '<i>CONFIGURATION_DETA</i> <i>ILS</i> ' mancante per le attività in TaskDefinition - ' <i>TASK_DEFINITION</i> '	I problemi di configurazione della rete possono verificarsi a causa della configurazione VPC mancante o di sottoreti mancanti o vuote. Verifica che la configurazione di rete sia corretta. Per ulteriori informazioni, consulta Prerequisiti per l'accesso all'immagine del contenitore. Per ulteriori informazioni, consulta i parametri di definizione delle attività di Amazon ECS nella Amazon Elastic Container Service Developer Guide.
	Le attività avviate quando i cluster avevano un tag di esclusione sono escluse dal Runtime Monitoring. ID attività interessati: '<i>TASK_ID</i>	Quando modifichi il GuardDuty tag predefinito da GuardDuty Managed - true a GuardDutyManaged -false, non GuardDuty riceverà gli eventi di runtime per questo cluster Amazon ECS. Aggiorna il tag a GuardDuty Managed - true e quindi riavvia l'attività.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	I servizi distribuiti quando i cluster avevano il tag di esclusione sono esclusi dal Runtime Monitoring. Nome/i dei servizi interessati: "<i>SERVICE_NAME</i>"	Quando i servizi distribuiti con il tag di esclusione e GuardDutyManaged -false, non GuardDuty riceveranno eventi di runtime per questo cluster Amazon ECS. Aggiorna il tag a GuardDutyManaged - true e quindi ridistribuisci il servizio.
	Le attività avviate prima dell'attivazione della configurazione automatica dell'agente non sono coperte. ID attività interessati: "<i>TASK_ID</i>"	Se il cluster contiene un'attività avviata prima di abilitare la configurazione automatizzata dell'agente per Amazon ECS, non GuardDuty sarà in grado di proteggerla. Riavvia l'attività affinché venga monitorata da GuardDuty
	I servizi distribuiti prima di abilitare la configurazione automatica degli agenti non sono coperti. Nome/i dei servizi interessati: "<i>SERVICE_NAME</i>"	Quando i servizi vengono distribuiti prima di abilitare la configurazione automatizzata degli agenti per Amazon ECS, non GuardDuty riceverà eventi di runtime per i cluster ECS.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	Il servizio '<i>SERVICE_NAME</i>' richiede una nuova implementazione per la correzione e la risoluzione dei problemi. Consulta la documentazione, Nome/i dei servizi interessati: "<i>SERVICE_NAME</i>	Un servizio avviato prima dell'attivazione del Runtime Monitoring non è supportato. Puoi riavviare il servizio o aggiornarlo con l'<code>forceNewDeployment</code> opzione seguendo i passaggi riportati in Aggiornamento di un servizio Amazon ECS utilizzando la console nella Amazon Elastic Container Service Developer Guide. In alternativa, puoi anche utilizzare i passaggi riportati UpdateServices nel riferimento all'API di Amazon Elastic Container Service.
	Le attività avviate prima di abilitare il Runtime Monitoring richiedono un riavvio. ID attività interessati: "<i>TASK_ID_1</i>	In Amazon ECS, le attività sono immutabili. Per valutare il comportamento di runtime o un' AWS Fargate attività in esecuzione, assicurati che Runtime Monitoring sia già abilitato, quindi riavvia l'attività per GuardDuty aggiungere il sidecar del contenitore.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Altri	Problema non identificato, per le attività in TaskDefinition - ' <i>TASK_DEFINITION</i> '	Utilizza le seguenti domande per identificare la causa principale del problema: • L'attività è iniziata prima di abilitare il Runtime Monitoring? In Amazon ECS, le attività sono immutabili. Per valutare il comportamento di runtime di un'attività Fargate in esecuzione, assicuratevi che Runtime Monitoring sia già abilitato, quindi riavviate l'attività per GuardDuty aggiungere il sidecar del contenitore. • Questa attività fa parte di una distribuzione di servizi iniziata prima di abilitare il Runtime Monitoring? In caso affermativo, è possibile riavviare il servizio o aggiornarlo <code>forceNewDeployment</code> utilizzando la procedura descritta in Aggiornamento di un servizio. Puoi anche usare UpdateService o AWS CLI.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		• L'attività è stata avviata dopo aver escluso il cluster ECS dal Runtime Monitoring? Quando si modifica il GuardDuty tag predefinito da GuardDutyManaged - true a GuardDutyManaged -false, non GuardDuty riceverà gli eventi di runtime per il cluster ECS. • Il tuo servizio contiene un'attività che ha un vecchio formato di? taskArn GuardDuty Runtime Monitoring non supporta la copertura per le attività che hanno il vecchio formato di taskArn. Per informazioni su Amazon Resource Names (ARNs) per le risorse Amazon ECS, consulta Amazon Resource Names (ARNs) e IDs.

Copertura del runtime e risoluzione dei problemi per i cluster Amazon EKS

Dopo aver abilitato il Runtime Monitoring e installato il GuardDuty security agent (componente aggiuntivo) per EKS manualmente o tramite la configurazione automatica degli agenti, puoi iniziare a valutare la copertura per i tuoi cluster EKS.

Indice

- [Revisione delle statistiche di copertura](#)
- [Modifica dello stato della copertura con EventBridge notifiche](#)
- [Risoluzione dei problemi di copertura del runtime di Amazon EKS](#)

Revisione delle statistiche di copertura

Le statistiche di copertura per i cluster EKS associati ai tuoi account o ai tuoi account membri consistono nella percentuale dei cluster EKS integri rispetto a tutti i cluster EKS nella Regione AWS selezionata. L'equazione seguente rappresenta questa percentuale come:

$$(\text{Cluster sani}) * 100 \text{ clusters} / \text{All}$$

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
- Nel riquadro di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Copertura runtime dei cluster EKS.
- Nella scheda Copertura runtime del cluster EKS puoi visualizzare le statistiche di copertura aggregate per stato di copertura, disponibili nella tabella Elenco cluster.
 - Puoi filtrare la tabella Elenco cluster in base alle seguenti colonne:
 - Nome cluster
 - ID account
 - Tipo di gestione dell'agente
 - Stato copertura
 - Versione del componente aggiuntivo
 - Se uno dei tuoi cluster EKS ha lo Stato copertura impostato su Non integro, la colonna Problema può includere informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Esegui l'[ListCoverage](#) API con il tuo ID rilevatore, la tua regione e l'endpoint di servizio validi. Puoi filtrare e ordinare l'elenco dei cluster utilizzando l'API in questione.
- Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `ADDON_VERSION`
 - `MANAGEMENT_TYPE`
- Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `ISSUE`
 - `ADDON_VERSION`
 - `UPDATED_AT`
- È possibile modificare *max-results* (fino a 50).
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui 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
```

- Esegui l'[GetCoverageStatistics](#) API per recuperare le statistiche aggregate sulla copertura basate su `statisticsType`
- Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:

- `COUNT_BY_COVERAGE_STATUS`: rappresenta le statistiche di copertura per i cluster EKS aggregate per stato di copertura.
- `COUNT_BY_RESOURCE_TYPE`— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
- È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `ADDON_VERSION`
 - `MANAGEMENT_TYPE`
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

```
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"}}] }'
```

Se lo stato di copertura del cluster EKS è Non integro, consulta [Risoluzione dei problemi di copertura del runtime di Amazon EKS](#).

Modifica dello stato della copertura con EventBridge notifiche

Lo stato di copertura di un cluster EKS nel tuo account potrebbe essere visualizzato come Non integro. Per rilevare quando lo stato di copertura diventa Non integro, ti consigliamo di monitorarlo periodicamente e di risolvere i problemi se è Non integro. In alternativa, puoi creare una EventBridge regola Amazon per avvisarti quando lo stato della copertura cambia Unhealthy da Healthy o in altro modo. Per impostazione predefinita, GuardDuty lo pubblica nel [EventBridge bus](#) per il tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta [Create rule](#) nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura del tuo cluster Amazon EKS cambia da Healthy aUnhealthy, detail-type dovresti farlo *GuardDuty Runtime Protection Unhealthy*. Per ricevere una notifica quando lo stato della copertura cambia da Unhealthy aHealthy, sostituisci il valore di detail-type con *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione 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"
  }
}
```

Risoluzione dei problemi di copertura del runtime di Amazon EKS

Se lo stato di copertura per il tuo cluster EKS è `Unhealthy`, puoi visualizzare l'errore corrispondente nella colonna Problema della GuardDuty console o utilizzando il tipo di [CoverageResource](#) dati.

Quando utilizzi tag di inclusione o di esclusione per monitorare in modo selettivo i cluster EKS, la sincronizzazione dei tag potrebbe richiedere del tempo. Ciò potrebbe influire sullo stato di copertura del cluster EKS associato. Puoi provare a rimuovere e aggiungere nuovamente il tag corrispondente (di inclusione o di esclusione). Per ulteriori informazioni, consulta [Assegnazione di tag alle risorse Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

La struttura di un problema di copertura è `Issue type:Extra information`. In genere, in caso di problemi vengono fornite Informazioni supplementari facoltative che possono includere specifiche eccezioni o descrizioni del problema sul lato client. Sulla base di informazioni aggiuntive, le tabelle seguenti forniscono i passaggi consigliati per risolvere i problemi di copertura per i cluster EKS.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Creazione del componente aggiuntivo non riuscita	L'addon non <code>aws-guard-duty-agent</code> è compatibile con la versione corrente del cluster. <i>ClusterName</i> Il componente aggiuntivo specificato non è supportato.	Assicurati di utilizzare una delle versioni di Kubernetes che supportano l'implementazione del componente aggiuntivo EKS <code>aws-guardduty-agent</code> . Per ulteriori informazioni, consulta Versioni di Kubernetes supportate dal security agent GuardDuty . Per informazioni sull'aggiornamento della versione di Kubernetes, consulta Aggiornamento di una versione Kubernetes del cluster Amazon EKS .
Creazione del componente aggiuntivo non riuscita	Problema relativo al componente aggiuntivo	Per informazioni sui passaggi consigliati per un codice di problema specifico del

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Aggiornamento del component e aggiuntivo non riuscito Stato del componente aggiuntivo non integro	EKS - AddonIssueCode : AddonIssueMessage	componente aggiuntivo, consulta. Troubleshooting steps for Addon creation/updatation error with Addon issue code Per un elenco dei codici di problema relativi ai componenti aggiuntivi che potresti riscontrare in questo problema, consulta. AddonIssue
Creazione degli endpoint VPC non riuscita	La creazione di endpoint VPC non è supportata per VPC condiviso <i>vpcId</i> Solo quando si utilizza un VPC condiviso con configurazione automatica degli agenti L'ID dell'account proprietario <i>111122223333</i> per il VPC condiviso <i>vpcId</i> non ha né il monitoraggio del runtime né la configurazione automatica degli agenti abilitati o entrambi.	Il Runtime Monitoring ora supporta l'uso di un VPC condiviso all'interno di un'organizzazione. Assicurati che i tuoi account soddisfino tutti i prerequisiti. Per ulteriori informazioni, consulta Prerequisiti per l'utilizzo di un VPC condiviso. L'account proprietario del VPC condiviso deve abilitare il monitoraggio del runtime e la configurazione automatica a degli agenti per almeno un tipo di risorsa (Amazon EKS o Amazon ECS ())AWS Fargate. Per ulteriori informazioni, consulta Prerequisiti specifici per il monitoraggio del runtime GuardDuty.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	L'abilitazione del DNS privato richiede entrambi <code>enableDnsSupport</code> e gli attributi <code>enableDnsHostnames</code> del VPC impostati <code>true</code> su <code>vpcId</code> for (Service: Ec2, Status Code:400, Request ID:). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>	Assicurati che i seguenti attributi VPC siano impostati su <code>true</code> – <code>enableDnsSupport</code> e <code>enableDnsHostnames</code> . Per ulteriori informazioni, consulta Attributi DNS nel VPC. Se utilizzi la console Amazon VPC su https://console.aws.amazon.com/vpc/ per creare Amazon VPC, assicurati di selezionare sia <code>Abilita nomi host DNS</code> che <code>Abilita risoluzione DNS</code>. Per ulteriori informazioni, consulta Opzioni di configurazione del VPC.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Eliminazione degli endpoint VPC condivisi non riuscita	L'eliminazione dell'endpoint VPC condiviso non è consentita per ID account, VPC 111122223333 <i>vpcId</i> condiviso, ID account proprietario. 555555555555	Potenziati passaggi: - La disabilitazione dello stato di monitoraggio del runtime dell'account partecipante VPC condiviso non influisce sulla policy degli endpoint VPC condivisi e sul gruppo di sicurezza esistente nell'account del proprietario. Per eliminare l'endpoint VPC condiviso e il gruppo di sicurezza, devi disabilitare il monitoraggio del runtime o lo stato di configurazione automatica dell'agente nell'account proprietario del VPC condiviso. - L'account partecipante VPC condiviso non può eliminare l'endpoint VPC condiviso e il gruppo di sicurezza ospitati nell'account proprietario del VPC condiviso.
Cluster EKS locali	I componenti aggiuntivi EKS non sono supportati sui cluster outpost locali.	Non utilizzabile. Per ulteriori informazioni, consulta Amazon EKS on AWS outposts.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Autorizzazione per l'abilitazione del monitoraggio del runtime EKS non concessa	(può mostrare o meno informazioni aggiuntive)	1. Se sono disponibili informazioni supplementari per questo problema, correggine la causa principale e segui la fase successiva. 2. Disattiva il monitoraggio del runtime EKS, quindi riattivalo. Assicurati che anche l' GuardDuty agente venga distribuito, automaticamente GuardDuty o manualmente.
Provisioning delle risorse per l'abilitazione del monitoraggio del runtime EKS in corso	(può mostrare o meno informazioni aggiuntive)	Non utilizzabile. Dopo aver abilitato il monitoraggio del runtime EKS, lo stato di copertura potrebbe rimanere Unhealthy fino al completamento della fase di provisioning delle risorse. Lo stato di copertura viene monitorato e aggiornato periodicamente.
Altri (qualsiasi altro problema)	Errore dovuto a un errore di autorizzazione	Disattiva il monitoraggio del runtime EKS, quindi riattivalo. Assicurati che anche l' GuardDuty agente venga distribuito, automaticamente GuardDuty o manualmente.

Procedura di risoluzione dei problemi relativi all' creation/updation errore Addon con codice di problema di Addon

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
Problema relativo all'addon <code>EKSInsufficientNumberofReplicas</code> : il component e aggiuntivo non è integro perché non ha il numero di repliche desiderato.	- Utilizzando il messaggio di problema, è possibile identificare e correggere la causa principale. Puoi iniziare descrivendo il tuo cluster. Ad esempio, kubectl describe pods da utilizzare per identificare la causa principale dell'errore del pod. Dopo aver corretto la causa principale, riprova il passaggio (creazione o aggiornamento del componente aggiuntivo). - Se il problema persiste, verifica che l'endpoint VPC per il tuo cluster Amazon EKS sia configurato correttamente. Per ulteriori informazioni, consulta Convalida della configurazione degli endpoint VPC.
Problema relativo al componente aggiuntivo <code>EKSInsufficientNumberofReplicas</code> : Il componente aggiuntivo non è integro perché uno o più pod non sono pianificati. Sono disponibili nodi: <code>0/x x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never</code>	Per risolvere il problema, è possibile procedere in uno dei seguenti modi: Aggiorna la priorità del pod dell' GuardDuty agente: Parametri e valori configurabili impostandola su una qualsiasi delle opzioni che supportano il valore <code>as. PriorityClass preemptionPolicy PreemptLowerPriority</code> Per informazioni sulla priorità dei pod, consulta Pod Priority e Preemption nella documentazione di Kubernetes.
Problema relativo al componente aggiuntivo <code>EKS-InsufficientNumberofReplicas</code> : Il componente aggiuntivo non è integro perché uno o più pod non sono pianificati. Sono disponibili nodi: <code>0/x x Too many pods.</code>	Scalabilità dell'istanza: per gestire le risorse e effettuare una selezione ottimale delle

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
preemption: not eligible due to preemptionPolicy=Never EKS Addon Issue -InsufficientNumber OfReplicas : Il componente aggiuntiv o non è integro perché uno o più pod non sono pianificati. Sono disponibili nodi:. 0/x 1 Insufficient memory. preemptio n: not eligible due to preemptio nPolicy=Never	istanze, consulta Gestire le risorse di calcolo utilizzando i nodi e Scegliere un tipo di istanza di nodo Amazon EC2 ottimale nella Guida per l'utente di Amazon EKS.  Note Il messaggio viene visualizzato o/ x perché GuardDuty riporta solo il primo errore rilevato. Il numero effettivo di pod in esecuzione nel GuardDuty daemonset potrebbe essere maggiore di 0.

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
EKS Addon Issue -InsufficientNumber OfReplicas : Il componente aggiuntivo non è salutare perché uno o più pod hanno contenitori in attesa CrashLoopBackOff: Completed	Puoi visualizzare i log associati al pod e identificare il problema. Per informazioni su come eseguire questa operazione, consulta Debug Running Pods nella documentazione di Kubernetes. Utilizza la seguente lista di controllo per risolvere questo problema relativo al componente aggiuntivo: • Verifica che il Runtime Monitoring sia abilitato . • Verifica che le distribuzioni del sistema operativoPrerequisiti per il supporto dei cluster Amazon EKS, ad esempio le distribuz ioni verificate del sistema operativo e le versioni Kubernetes supportate, siano soddisfatte. • Quando gestisci manualmente il security agent, conferma di aver creato un endpoint VPC per tutti. VPCs Quando abiliti la configurazione GuardDuty automatizzata, dovresti comunque verificare che l'endpoin t VPC venga creato. Ad esempio, quando si utilizza un VPC condiviso in configurazione automatizzata. Per convalidarlo, consulta. Convalida della configurazione degli endpoint VPC • Verifica che il GuardDuty security agent sia in grado di risolvere il DNS privato dell'endpoint GuardDuty VPC. Per conoscere gli endpoint,

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
	consulta Nomi DNS privati per gli endpoint in. Gestione degli agenti GuardDuty di sicurezza A tale scopo, puoi utilizzare nslookup uno strumento su Windows o Mac o uno dig strumento su Linux. Quando usi nslookup, puoi usare il seguente comando dopo aver sostituito la regione <i>us-west-2</i> con la tua regione: <pre>nslookup guardduty-data. <i>us-west-2</i>.amazonaws.com</pre> • Verifica che la policy degli endpoint GuardDuty VPC o la policy di controllo del servizio non influiscano sulle azioni. <code>guardduty:SendSecurityTelemetry</code>

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
EKS Addon Issue -InsufficientNumber OfReplicas : Il componente aggiuntivo non è salutare perché in uno o più pod sono presenti contenitori in attesa CrashLoop BackOff: Error	Puoi visualizzare i log associati al pod e identificare il problema. Per informazioni su come eseguire questa operazione, consulta Debug Running Pods nella documentazione di Kubernetes. Dopo aver identificato il problema, utilizza la seguente lista di controllo per risolverlo: • Verifica che il Runtime Monitoring sia abilitato . • Verifica che le distribuzioni del sistema operativo Prerequisiti per il supporto dei cluster Amazon EKS, ad esempio le distribuz ioni verificate del sistema operativo e le versioni Kubernetes supportate, siano soddisfatte. • Il GuardDuty security agent è in grado di risolvere il DNS privato dell'endpoint GuardDuty VPC. Per conoscere gli endpoint, vedi Nomi DNS privati per gli endpoint in. Gestione degli agenti GuardDuty di sicurezza
EKS Addon Issue AdmissionRequestDe nied : webhook di ammissione "validate .kyverno.svc-fail" ha negato la richiesta: policy DaemonSet/amazon-g uardduty/aws-guardduty-agent per la violazione delle risorse::..... restrict-image-reg istries autogen-validate-registries	1. Il cluster Amazon EKS o l'amministratore della sicurezza devono rivedere la politica di sicurezza che blocca l'aggiornamento dell'Addon. 2. Devi disabilitare il controller (webhook) o fare in modo che il controller accetti le richieste da Amazon EKS.

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
EKS Addon Issue -ConfigurationConflict : Conflitti rilevati durante il tentativo di candidatura. Non continuerà a causa della modalità di risoluzione dei conflitti. Conflicts: DaemonSet.apps aws-guarddduty-agent - .spec.template.spec.containers[name="aws-guarddduty-agent"].image	Quando crei o aggiorni l'Addon, fornisci il flag di OVERWRITE risoluzione del conflitto. Ciò potrebbe sovrascrivere qualsiasi modifica apportata direttamente alle risorse correlate in Kubernetes utilizzando l'API Kubernetes. Puoi prima rimuovere un componente aggiuntivo o Amazon EKS da un cluster e poi reinstallarlo.

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
Problema relativo al componente aggiuntivo EKS - AccessDenied: priorityclasses.scheduling.k8s.io "aws-guarddduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope AddonUpdationFailed: EKSAaddon Problema - AccessDenied: namespaces\"amazon-guarddduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guarddduty\"	È necessario aggiungere l'autorizzazione mancante al eks:addon-cluster-admin ClusterRoleBinding manuale. Aggiungi quanto segue yaml aeks:addon-cluster-admin : <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> Ora puoi applicarlo yaml al tuo cluster Amazon EKS utilizzando il seguente comando: <pre>kubectl apply -f eks-addon-cluster-admin.yaml</pre>

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
Problema aggiuntivo EKS - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label	È necessario disabilitare il controller o fare in modo che il controller accetti le richieste dal cluster Amazon EKS. Prima di creare o aggiornare il componente aggiuntivo, puoi anche creare uno spazio dei GuardDuty nomi ed etichettarlo come. owner
Problema relativo al componente aggiuntivo EKS - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label	È necessario disabilitare il controller o fare in modo che il controller accetti le richieste dal cluster Amazon EKS. Prima di creare o aggiornare il componente aggiuntivo, puoi anche creare uno spazio dei GuardDuty nomi ed etichettarlo come. owner
Problema relativo al componente aggiuntivo EKS - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container-registries] container <aws-guardduty-agent> has an invalid image registry	Aggiungi il registro delle immagini per GuardDuty al tuo controller allowed-container-registries di ammissione. Per ulteriori informazioni, consultate il repository ECR per EKS v1.8.1-eks-build.2 in. Agente di hosting del repository Amazon ECR GuardDuty

Configurazione del monitoraggio della CPU e della memoria

Dopo aver abilitato il monitoraggio del runtime e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di analisi.

I seguenti argomenti possono aiutarti a valutare le prestazioni dell'agente distribuito rispetto ai limiti di CPU e memoria dell' GuardDuty agente.

Configurazione del monitoraggio sul cluster Amazon ECS

I seguenti passaggi della Amazon CloudWatch User Guide possono aiutarti a valutare le prestazioni dell'agente distribuito rispetto ai limiti di CPU e memoria per l' GuardDuty agente:

1. [Configurazione di Container Insights su Amazon ECS per parametri a livello di cluster e servizio](#)
2. [Parametri di Amazon ECS Container Insights](#)

Configurazione del monitoraggio sul cluster Amazon EKS

Dopo aver implementato il GuardDuty security agent e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di Container Insight.

Valuta le prestazioni del security agent

1. [Configurazione di Container Insights su Amazon EKS e Kubernetes](#) nella Amazon User Guide CloudWatch
2. [Parametri di Amazon EKS e Kubernetes Container Insights nella](#) Amazon User Guide CloudWatch

Gestisci le prestazioni con Security Agent v1.5.0 e versioni successive

Con Security Agent [v1.5.0 e versioni successive](#), quando gli approfondimenti indicano che l' GuardDuty agente associato sta raggiungendo i limiti assegnati, puoi configurare parametri specifici. Per ulteriori informazioni, consulta [Configura i parametri aggiuntivi EKS](#).

Utilizzo di un VPC condiviso con Runtime Monitoring

GuardDuty Il Runtime Monitoring supporta l'utilizzo di Amazon Virtual Private Cloud (Amazon VPC) condiviso per i tuoi Account AWS utenti che appartengono alla stessa organizzazione in. AWS Organizations Puoi usare un VPC condiviso in due modi:

- Configurazione automatica dell'agente (consigliata): quando gestisce GuardDuty automaticamente il security agent, configura anche la policy degli endpoint Amazon VPC. Questa politica si basa sulle impostazioni VPC condivise dell'organizzazione.

È necessario abilitare la configurazione automatica degli agenti nell'account proprietario del VPC condiviso e in tutti gli account partecipanti che condivideranno questo VPC.

- **Agente gestito manualmente:** quando gestisci manualmente il security agent con un VPC condiviso, devi aggiornare la policy degli endpoint VPC per consentire agli account corrispondenti di accedere al VPC condiviso. A tale scopo, è possibile utilizzare la politica di esempio condivisa nella sezione seguente. [Come funziona](#)

Per gli scenari di gestione manuale che coinvolgono account partecipanti per un VPC condiviso, lo stato della copertura potrebbe non essere accurato. Per garantire up-to-date la protezione e lo stato di copertura delle risorse, GuardDuty consiglia di abilitare la configurazione automatica degli agenti per tutti gli account che utilizzeranno un VPC condiviso.

Argomenti

- [Come funziona](#)
- [Prerequisiti per l'utilizzo di un VPC condiviso](#)

Come funziona

Anche le persone Account AWS che appartengono alla stessa organizzazione dell'account proprietario Amazon VPC condiviso possono condividere lo stesso endpoint Amazon VPC. Ciascuno degli account che utilizzano la stessa policy per gli endpoint di Amazon VPC viene chiamato AWS account partecipante dell'Amazon VPC condiviso associato.

L'esempio seguente mostra la politica degli endpoint VPC predefinita dell'account proprietario del VPC condiviso e dell'account partecipante. `aws:PrincipalOrgID` mostrerà l'ID dell'organizzazione associato alla risorsa VPC condivisa. L'uso di questa politica è limitato agli account dei partecipanti presenti nell'organizzazione dell'account del proprietario.

Example Esempio di policy di endpoint VPC condivisa

JSON

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



```
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalOrgID": "o-abcdef0123"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

Con configurazione GuardDuty automatica degli agenti

Quando l'account proprietario del VPC condiviso abilita il monitoraggio del runtime e la configurazione automatica degli agenti per una qualsiasi delle risorse (Amazon EKS o (solo AWS Fargate Amazon ECS)), tutte le risorse condivise VPCs diventano idonee per l'installazione automatica dell'endpoint Amazon VPC condiviso e del gruppo di sicurezza associato nell'account proprietario del VPC condiviso. GuardDuty recupera l'ID dell'organizzazione associato all'Amazon VPC condiviso.

GuardDuty crea un endpoint Amazon VPC quando l'account proprietario del VPC condiviso o l'account partecipante ne hanno bisogno. Esempi di necessità di un endpoint Amazon VPC includono l' GuardDutyattivazione, il monitoraggio del runtime, il monitoraggio del runtime EKS o il lancio di una nuova attività Amazon ECS-Fargate. Quando questi account abilitano il Runtime Monitoring e la configurazione automatizzata degli agenti per qualsiasi tipo di risorsa, GuardDuty creano un endpoint Amazon VPC e impostano la policy dell'endpoint con lo stesso ID dell'organizzazione dell'account proprietario del VPC condiviso. GuardDuty aggiunge un GuardDutyManaged tag e lo imposta `true` per l'endpoint Amazon VPC che lo crea. GuardDuty Se l'account proprietario di Amazon VPC condiviso non ha abilitato il monitoraggio del runtime o la configurazione automatica degli agenti per nessuna delle risorse, non GuardDuty imposterà la policy degli endpoint di Amazon VPC. Per informazioni sulla configurazione del Runtime Monitoring e sulla gestione automatica del security agent nell'account proprietario del VPC condiviso, consulta. [Abilitazione del monitoraggio del GuardDuty runtime](#)

Utilizzo con un agente gestito manualmente

Quando utilizzi un VPC condiviso con un agente gestito manualmente, verifica che non esista una policy esplicita sugli Deny endpoint che blocchi gli account che devono utilizzare il VPC condiviso. Ciò impedirà al Security Agent di inviare dati di telemetria a, con conseguente stato di copertura. GuardDuty Unhealthy Per configurare la politica degli endpoint, vedere. [Example shared VPC endpoint policy](#)

La copertura del runtime potrebbe non essere accurata in scenari come la mancanza di autorizzazioni per il VPC condiviso. È possibile monitorare continuamente la copertura delle risorse seguendo i passaggi relativi al tipo di risorsa. [Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi](#)

Per garantire la protezione continua del Runtime Monitoring delle risorse di elaborazione, GuardDuty consiglia di abilitare la configurazione automatizzata degli agenti per l'account proprietario del VPC condiviso e tutti gli account partecipanti per le tue risorse.

Prerequisiti per l'utilizzo di un VPC condiviso

Come parte della configurazione iniziale, esegui i seguenti passaggi se desideri diventare il proprietario del VPC condiviso: Account AWS

1. Creazione di un'organizzazione: crea un'organizzazione seguendo i passaggi descritti in [Creazione e gestione di un'organizzazione](#) nella Guida per l'AWS Organizations utente.

Per informazioni sull'aggiunta o la rimozione degli account dei membri, consulta [Gestione Account AWS nell'organizzazione](#).

2. Creazione di una risorsa VPC condivisa: puoi creare una risorsa VPC condivisa dall'account del proprietario. Per ulteriori informazioni, consulta [Condividi le tue sottoreti VPC con altri account nella](#) Amazon VPC User Guide.

Prerequisiti specifici per il monitoraggio del runtime GuardDuty

L'elenco seguente fornisce i prerequisiti specifici per: GuardDuty

- L'account proprietario del VPC condiviso e l'account partecipante possono appartenere a organizzazioni diverse in. GuardDuty Tuttavia, devono appartenere alla stessa organizzazione in AWS Organizations. Ciò è necessario per GuardDuty creare un endpoint Amazon VPC e un

gruppo di sicurezza per il VPC condiviso. Per informazioni su come VPCs funziona la condivisione, consulta [Condividi il tuo VPC con altri account](#) nella Amazon VPC User Guide.

- Abilita Runtime Monitoring o EKS Runtime Monitoring e la configurazione GuardDuty automatica degli agenti per qualsiasi risorsa nell'account proprietario del VPC condiviso e nell'account partecipante. Per ulteriori informazioni, consulta [Abilitazione del monitoraggio del runtime](#).

Se hai già completato queste configurazioni, continua con il passaggio successivo.

- Quando lavori con un'attività Amazon EKS o Amazon ECS (AWS Fargate solo), assicurati di scegliere la risorsa VPC condivisa associata all'account del proprietario e di selezionarne le sottoreti.

Utilizzo di Infrastructure as Code (IaC) con agenti di sicurezza automatizzati GuardDuty

Utilizza questa sezione solo se il seguente elenco si applica al tuo caso d'uso:

- Utilizzate strumenti Infrastructure as Code (IaC), come Terraform, per gestire AWS le vostre risorse AWS Cloud Development Kit (AWS CDK) e
- È necessario abilitare la configurazione GuardDuty automatica degli agenti per uno o più tipi di risorse: Amazon EKS, Amazon EC2 o Amazon ECS-Fargate.

Panoramica del grafico sulla dipendenza delle risorse IaC

Quando abiliti la configurazione GuardDuty automatica dell'agente per un tipo di risorsa, crea GuardDuty automaticamente un endpoint VPC e un gruppo di sicurezza associati a questo endpoint VPC e installa il security agent per questo tipo di risorsa. Per impostazione predefinita, GuardDuty eliminerà l'endpoint VPC e il gruppo di sicurezza associato solo dopo aver disabilitato il Runtime Monitoring. Per ulteriori informazioni, consulta [Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring](#).

Quando si utilizza uno strumento IaC, questo mantiene un grafico delle dipendenze delle risorse. Al momento dell'eliminazione delle risorse utilizzando lo strumento IaC, elimina solo le risorse che possono essere tracciate come parte del grafico delle dipendenze delle risorse. Gli strumenti IaC potrebbero non conoscere le risorse create al di fuori della configurazione specificata. Ad esempio, si crea un VPC con uno strumento IaC e quindi si aggiunge un gruppo di sicurezza a questo VPC utilizzando la AWS console o un'operazione API. Nel grafico delle dipendenze delle risorse, la risorsa

VPC creata dipende dal gruppo di sicurezza associato. Se elimini questa risorsa VPC utilizzando lo strumento IAc, riceverai un errore. Il modo per aggirare questo errore consiste nell'eliminare manualmente il gruppo di sicurezza associato o nell'aggiornare la configurazione IAc per includere questa risorsa aggiunta.

Problema comune: eliminazione di risorse in IAc

Quando utilizzi la configurazione GuardDuty automatizzata degli agenti, potresti voler eliminare una risorsa (Amazon EKS, Amazon EC2 o Amazon ECS-Fargate) creata utilizzando uno strumento IAc. Tuttavia, questa risorsa dipende dall'endpoint VPC creato. GuardDuty Ciò impedisce allo strumento IAc di eliminare la risorsa da solo e richiede di disabilitare il Runtime Monitoring, che elimina ulteriormente l'endpoint VPC automaticamente.

Ad esempio, quando tenti di eliminare l'endpoint VPC GuardDuty creato per tuo conto, riceverai un errore simile agli esempi seguenti.

Example

Esempio di errore quando si utilizza CDK

The following resource(s) failed to delete:

```
[mycdkvpapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpapplicationprivatesubnet1Subnet1SubnetEXAMPLE1]  
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-8357-5557b7EXAMPLE)  
HandlerErrorCode: InvalidRequest)
```

Example

Esempio di errore durante l'utilizzo di 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
```

Soluzione: prevenire il problema dell'eliminazione delle risorse

Questa sezione ti aiuta a gestire l'endpoint VPC e il gruppo di sicurezza indipendentemente da GuardDuty.

Per ottenere la proprietà completa delle risorse configurate utilizzando lo strumento IaC, effettuate le seguenti operazioni nell'ordine elencato:

1. Crea un VPC. Per consentire l'autorizzazione di ingresso, associa un endpoint GuardDuty VPC al gruppo di sicurezza, a questo VPC.
2. Abilita la configurazione GuardDuty automatica degli agenti per il tuo tipo di risorsa.

Dopo aver completato i passaggi precedenti, non GuardDuty creerà il proprio endpoint VPC e riutilizzerà quello creato utilizzando lo strumento IaC.

Per informazioni sulla creazione del tuo VPC, consulta [Creare un VPC solo negli Amazon VPC Transit Gateway](#). Per informazioni sulla creazione di un endpoint VPC, consulta la sezione seguente per il tipo di risorsa:

- Per Amazon EC2, vedi [Prerequisito: creazione manuale di un endpoint Amazon VPC](#).
- Per Amazon EKS, vedi [Prerequisito: creazione di un endpoint Amazon VPC](#).

Tipi di eventi di runtime raccolti che GuardDuty utilizzano

Il GuardDuty security agent raccoglie i seguenti tipi di eventi e li invia al GuardDuty backend per il rilevamento e l'analisi delle minacce. GuardDuty non rende questi eventi accessibili all'utente. Se GuardDuty rileva una potenziale minaccia e genera una [Tipi di risultati del monitoraggio del runtime](#), puoi visualizzare i dettagli del ritrovamento corrispondenti.

Per informazioni su come GuardDuty utilizza i tipi di eventi raccolti in Runtime Monitoring, vedere [Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio](#).

Eventi di processo

Gli eventi di processo rappresentano le informazioni associate ai processi in esecuzione su istanze Amazon EC2 e carichi di lavoro di container. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di processo che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Process name (Nome del processo)	Nome del processo osservato.
Percorso del processo	Percorso assoluto dell'eseguibile del processo.
ID processo	L'ID che il sistema operativo assegna al processo.
PID dello spazio dei nomi	L'ID del processo in uno spazio dei nomi PID secondario diverso dallo spazio dei nomi PID a livello di host. Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
ID utente del processo	L'ID univoco dell'utente che ha eseguito il processo.
UUID processo	L'ID univoco assegnato al processo da GuardDuty.
GID processo	L'ID processo del gruppo di processi.
EGID processo	L'ID di gruppo effettivo del gruppo di processi.
EUID processo	L'ID utente effettivo del processo.
Nome utente del processo	Il nome dell'utente che ha eseguito il processo.
Ora di inizio del processo	L'ora in cui è stato creato il processo. Questo campo è nel formato della stringa di data UTC (2023-03-22T19:37:20.168Z).
SHA-256 eseguibile del processo	L'hash SHA256 dell'eseguibile del processo.
Percorso dello script di processo	Il percorso del file di script che è stato eseguito.
Variabile di ambiente del processo	La variabile di ambiente messa a disposizione del processo. Vengono raccolti solo LD_PRELOAD e LD_LIBRARY_PATH .

Nome campo	Description
Directory di lavoro presente (PWD) del processo	La directory di lavoro presente del processo.
Processo padre	I dettagli del processo padre. Un processo padre è un processo che ha creato quello osservato.
Argomenti della riga di comando Attualmente, questo campo è limitato a versioni di agenti specifiche corrispondenti al tipo di risorsa: • Fargate (solo Amazon ECS) con GuardDuty security agent v1.0.0 e versioni successive. • Istanze Amazon EC2 con GuardDuty security agent v1.0.0 e versioni successive. • Cluster Amazon EKS con security agent v1.4.0 e versioni successive. Per ulteriori informazioni, consulta GuardDuty versioni di rilascio di Security Agent.	
	Argomenti della riga di comando forniti al momento dell'esecuzione del processo. Questo campo potrebbe contenere dati sensibili dei clienti.

Eventi del container

Gli eventi del contenitore rappresentano informazioni associate alle attività dei carichi di lavoro dei container. La tabella seguente include i nomi dei campi e le descrizioni degli eventi del carico di lavoro del contenitore che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Nome container	Il nome del container. Se disponibile, questo campo mostra il valore dell'etichetta <code>io.kubernetes.container.name</code>.

Nome campo	Description
UID Container	L'ID univoco del container assegnato dal runtime del container.
Runtime del container	Il runtime del container (ad esempio docker o containerd) utilizzato per eseguire il container.
ID immagine del container	L'ID dell'immagine del container.
Nome immagine del container	Il nome dell'immagine del container.

AWS Fargate (solo Amazon ECS) eventi relativi alle attività

Gli eventi delle attività Fargate-Amazon ECS rappresentano attività associate alle attività di Amazon ECS in esecuzione su computer Fargate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi delle attività di Amazon ECS-Fargate raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Nome risorsa Amazon (ARN) dell'attività	L'ARN dell'attività.
Nome del cluster	Il nome del cluster Amazon ECS.
Cognome	Cognome della definizione dell'attività. familyViene utilizzato come nome per la definizione dell'attività utilizzata per avviare l'attività.
Nome del servizio	Il nome del servizio Amazon ECS, se l'attività è stata avviata come parte di un servizio.
Tipo di lancio	L'infrastruttura su cui viene eseguita l'attività. Per Runtime Monitoring con tipo di risorsa asECSCluster , il tipo di avvio potrebbe essere EC2 oFARGATE.
CPU	Il numero di unità CPU utilizzate dall'attività, espresso nella definizione dell'attività.

Eventi pod di Kubernetes

La tabella seguente include i nomi dei campi e le descrizioni degli eventi del pod Kubernetes che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
ID pod	L'ID del pod di Kubernetes.
Nome pod	Il nome del pod di Kubernetes.
Spazio dei nomi pod	Il nome dello spazio dei nomi di Kubernetes a cui appartiene il carico di lavoro di Kubernetes.
Nome del cluster Kubernetes	Il nome del cluster Kubernetes.

Eventi del Domain Name System (DNS)

Gli eventi del Domain Name System (DNS) includono i dettagli delle query DNS effettuate dai tipi di risorse e le risposte corrispondenti. La tabella seguente include i nomi dei campi e le descrizioni degli eventi DNS raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, <code>SOCK_RAW</code> .
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi <code>AF_INET</code> viene utilizzata per il protocollo IPv4.
ID direzione	L'ID della direzione della connessione.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per l'UDP e 6 per il TCP.
IP dell'endpoint remoto DNS	L'IP remoto della connessione.

Nome campo	Description
Porta dell'endpoint remoto DNS	Il numero di porta della connessione.
IP dell'endpoint locale DNS	L'IP locale della connessione.
Porta dell'endpoint locale DNS	Il numero di porta della connessione.
Payload DNS	Il payload di pacchetti DNS che contiene query e risposte DNS.

Eventi aperti

Gli eventi aperti sono associati all'accesso e alla modifica dei file. La tabella seguente include i nomi dei campi e le descrizioni degli eventi aperti raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Percorso del file	Il percorso del file aperto in questo evento.
Flag	Descrive la modalità di accesso ai file, ad esempio sola lettura, sola scrittura e lettura e scrittura.

Evento modulo di caricamento

La tabella seguente include il nome del campo e la descrizione dell'evento del modulo di caricamento che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Nome del modulo	Il nome del modulo caricato nel kernel.

Eventi mprotect

Gli eventi Mprotect forniscono informazioni sulle modifiche alle impostazioni di protezione della memoria dei processi in esecuzione sui sistemi monitorati. La tabella seguente include i nomi dei campi e le descrizioni degli eventi Mprotect che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Intervallo di indirizzi	L'intervallo di indirizzi per il quale sono state modificate le protezioni di accesso.
Regioni di memoria	Specifica la regione dello spazio degli indirizzi di un processo, ad esempio stack e heap.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Eventi di montaggio

Gli eventi di montaggio forniscono informazioni associate al montaggio e allo smontaggio dei file system sulla risorsa monitorata. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di montaggio raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Destinazione di montaggio	Il percorso in cui è montata l'origine di montaggio.
Origine di montaggio	Il percorso sull'host montato sulla destinazione di montaggio.
Tipo di file system	Rappresenta il tipo di file system montato.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Eventi di collegamento

Gli eventi di collegamento forniscono visibilità sulle attività di gestione dei link del file system nelle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di collegamento raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Percorso di collegamento	Il percorso in cui viene creato il collegamento fisico.
Percorso di destinazione	Il percorso del file a cui punta il collegamento fisico.

Eventi collegamento simbolico

Gli eventi Symlink forniscono visibilità sulle attività di gestione dei link simbolici del file system nelle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi symlink raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Percorso di collegamento	Il percorso in cui viene creato il collegamento simbolico.
Percorso di destinazione	Il percorso del file a cui punta il collegamento simbolico.

Eventi dup

Gli eventi Dup forniscono visibilità sulla duplicazione dei descrittori di file da parte dei processi in esecuzione sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi dup raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Vecchio descrittore di file	Un descrittore di file che rappresenta un oggetto file aperto.
Nuovo descrittore di file	Un nuovo descrittore di file che è un duplicato di quello vecchio. Sia il descrittore di file vecchio che quello nuovo rappresentano lo stesso oggetto file aperto.

Nome campo	Description
IP dell'endpoint remoto dup	L'indirizzo IP remoto del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
Porta dell'endpoint remoto dup	La porta remota del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
IP dell'endpoint locale dup	L'indirizzo IP locale del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
Porta dell'endpoint locale dup	La porta locale del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.

Evento mappa di memoria

La tabella seguente include il nome del campo e la descrizione degli eventi della mappa di memoria raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Percorso del file	Il percorso del file su cui la memoria viene mappata.

Eventi socket

Gli eventi socket forniscono informazioni sulle connessioni socket di rete utilizzate nelle attività delle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi socket raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi AF_INET viene utilizzata per la versione IP del protocollo 4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, SOCK_RAW.
Numero di protocollo	Specifica un protocollo particolare all'interno della famiglia di indirizzi. In genere esiste un unico protocollo nelle famiglie di indirizzi. Ad esempio, la famiglia di indirizzi AF_INET ha solo il protocollo IP.

Connetti eventi

Gli eventi Connect forniscono visibilità sulle connessioni di rete stabilite dai processi sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di connessione raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi AF_INET viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, SOCK_RAW.
Numero di protocollo	Specifica un protocollo particolare all'interno della famiglia di indirizzi. In genere esiste un unico protocollo nelle famiglie di indirizzi. Ad esempio, la famiglia di indirizzi AF_INET ha solo il protocollo IP.
Percorso del file	Il percorso del file socket se la famiglia di indirizzi è AF_UNIX.
IP dell'endpoint remoto	L'IP remoto della connessione.

Nome campo	Description
Porta dell'endpoint remoto	Il numero di porta della connessione.
IP dell'endpoint locale	L'IP locale della connessione.
Porta dell'endpoint locale	Il numero di porta della connessione.

Eventi VM Readv processo

Gli eventi Process VM readv forniscono visibilità sulle operazioni di lettura eseguite dai processi nelle rispettive aree di memoria virtuale. La tabella seguente include i nomi dei campi e le descrizioni degli eventi readv delle macchine virtuali di processo che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.
PID di destinazione	L'ID processo del processo da cui viene letta la memoria.
UUID del processo di destinazione	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.

Eventi VM Writev processo

Gli eventi Process VM writev forniscono visibilità sulle operazioni di scrittura eseguite dai processi nelle rispettive aree di memoria virtuale. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di scrittura delle macchine virtuali di processo che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.
PID di destinazione	L'ID processo del processo su cui viene scritta la memoria.
UUID del processo di destinazione	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.

Eventi Process Trace (Ptrace)

La chiamata di sistema Process trace (Ptrace) è un meccanismo di debug e tracciamento che consente a un processo (tracer) di osservare e controllare l'esecuzione di un altro processo (tracee). Ciò fornisce al tracer la capacità di ispezionare e modificare la memoria, i registri e il flusso di esecuzione del processo di destinazione.

Gli eventi Ptrace forniscono visibilità sull'uso della chiamata di sistema ptrace da parte dei processi in esecuzione sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi ptrace che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
PID di destinazione	L'ID processo del processo di destinazione.
UUID del processo di destinazione	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Associa eventi

Gli eventi di associazione forniscono visibilità sull'associazione dei socket di rete mediante i processi in esecuzione sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di associazione raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi AF_INET viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, SOCK_RAW.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per l'UDP e 6 per il TCP.
IP dell'endpoint locale	L'IP locale della connessione.
Porta endpoint locale	Il numero di porta della connessione.

Ascolta gli eventi

Gli eventi di ascolto forniscono visibilità sullo stato di ascolto dei socket di rete, indicando se un socket di rete è pronto o meno ad accettare connessioni in entrata. Un processo in esecuzione sulla risorsa monitorata imposta il socket di rete in uno stato di ascolto. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di ascolto raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi AF_INET viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, SOCK_RAW.

Nome campo	Description
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per l'UDP e 6 per il TCP.
IP dell'endpoint locale	L'IP locale della connessione.
Porta endpoint locale	Il numero di porta della connessione.

Rinomina gli eventi

Gli eventi di ridenominazione forniscono informazioni sulla ridenominazione di file e directory in base ai processi in esecuzione sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi di ridenominazione raccolti da Runtime Monitoring per rilevare potenziali minacce.

Nome campo	Description
Percorso del file	Percorso in cui si trova il file che viene rinominato.
Target	Il nuovo percorso del file.

Imposta gli eventi relativi all'ID utente (UID)

Gli eventi Set user ID (UID) forniscono visibilità sulle modifiche apportate all'ID utente (UID) associato ai processi in esecuzione sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi UID impostati che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Nuovo EUID	Il nuovo ID utente effettivo del processo.
Nuovo UID	Il nuovo ID utente del processo.

Eventi Chmod

Gli eventi Chmod forniscono visibilità sulle modifiche nelle autorizzazioni (modalità) di file e directory sulle risorse monitorate. La tabella seguente include i nomi dei campi e le descrizioni degli eventi chmod che Runtime Monitoring raccoglie per rilevare potenziali minacce.

Nome campo	Description
Percorso del file	Percorso del file che richiama questo evento.
Modalità file	Le autorizzazioni di accesso aggiornate per il file associato.

Agente di hosting del repository Amazon ECR GuardDuty

Nelle sezioni seguenti sono elencati i repository Amazon Elastic Container Registry (Amazon ECR) GuardDuty in cui è ospitato l'agente di sicurezza che viene distribuito sui cluster Amazon EKS e Amazon ECS.

Il prerequisito [Prerequisiti per l'accesso all'immagine del contenitore](#) richiede di fornire un ruolo di esecuzione delle attività con determinate autorizzazioni Amazon Elastic Container Registry (Amazon ECR). Per limitare ulteriormente queste autorizzazioni, puoi aggiungere l'URI del repository Amazon ECR che ospita l' GuardDuty agente per le risorse Fargate-Amazon ECS.

Indice

- [Archivio ECR per le versioni dell'agente EKS 1.12.1 - 1.8.1 \(eks.build.2\)](#)
- [Repository ECR per l'agente EKS versione 1.8.1 \(\) eks.build.1](#)
- [Repository ECR per GuardDuty agente su \(solo AWS Fargate Amazon ECS\)](#)

Archivio ECR per le versioni dell'agente EKS 1.12.1 - 1.8.1 (eks.build.2)

Quando abiliti la configurazione GuardDuty automatizzata per Runtime Monitoring for EKS, GuardDuty distribuirà questa versione dell'agente nei tuoi cluster Amazon EKS. Per informazioni sull'attivazione dell'agente automatizzato, consulta. [Gestione automatica dell'agente di sicurezza per le risorse Amazon EKS](#)

La tabella seguente mostra il repository Amazon ECR URIs in cui sono ospitate le versioni del GuardDuty security agent 1.12.1.eks.build.2

1.11.0.eks.build.21.10.0.eks.build.2,1.9.0.eks.build.2, e per
1.8.0.eks.build.2 Amazon EKS.

Regione AWS	URI del repository Amazon ECR
Stati Uniti occidentali (Oregon)	602401143452.dkr.ecr.us-west-2.amazonaws.com
	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europa (Parigi)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia Pacifico (Mumbai)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pacifico (Hyderabad)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canada (Centrale)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Canada occidentale (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
	—

Regione AWS	URI del repository Amazon ECR
Medio Oriente (Emirati Arabi Uniti)	<code>759879836304.dkr.ecr.me-central-1.amazonaws.com</code>
	<code>601769779514.dkr.ecr.me-central-1.amazonaws.com</code>
Europa (Londra)	<code>602401143452.dkr.ecr.eu-west-2.amazonaws.com</code>
	<code>109118265657.dkr.ecr.eu-west-2.amazonaws.com</code>
Stati Uniti occidentali (California settentrionale)	<code>602401143452.dkr.ecr.us-west-1.amazonaws.com</code>
	<code>373421517865.dkr.ecr.us-west-1.amazonaws.com</code>
Stati Uniti orientali (Virginia settentrionale)	<code>602401143452.dkr.ecr.us-east-1.amazonaws.com</code>
	<code>031903291036.dkr.ecr.us-east-1.amazonaws.com</code>
Stati Uniti orientali (Ohio)	<code>602401143452.dkr.ecr.us-east-2.amazonaws.com</code>
	<code>591382732059.dkr.ecr.us-east-2.amazonaws.com</code>
Europa (Irlanda)	<code>602401143452.dkr.ecr.eu-west-1.amazonaws.com</code>
	<code>673884943994.dkr.ecr.eu-west-1.amazonaws.com</code>
Sud America (San Paolo)	<code>602401143452.dkr.ecr.sa-east-1.amazonaws.com</code>

Regione AWS	URI del repository Amazon ECR
	<code>941219317354.dkr.ecr.sa-east-1.amazonaws.com</code>
Europa (Stoccolma)	<code>602401143452.dkr.ecr.eu-north-1.amazonaws.com</code>
	<code>366771026645.dkr.ecr.eu-north-1.amazonaws.com</code>
Europa (Francoforte)	<code>602401143452.dkr.ecr.eu-central-1.amazonaws.com</code>
	<code>409493279830.dkr.ecr.eu-central-1.amazonaws.com</code>
Europa (Zurigo)	<code>900612956339.dkr.ecr.eu-central-2.amazonaws.com</code>
	<code>718440343717.dkr.ecr.eu-central-2.amazonaws.com</code>
Asia Pacifico (Singapore)	<code>602401143452.dkr.ecr.ap-southeast-1.amazonaws.com</code>
	<code>584580519942.dkr.ecr.ap-southeast-1.amazonaws.com</code>
Asia Pacifico (Sydney)	<code>602401143452.dkr.ecr.ap-southeast-2.amazonaws.com</code>
	<code>011662287384.dkr.ecr.ap-southeast-2.amazonaws.com</code>
Asia Pacifico (Giacarta)	<code>296578399912.dkr.ecr.ap-southeast-3.amazonaws.com</code>
	<code>617474730032.dkr.ecr.ap-southeast-3.amazonaws.com</code>

Regione AWS	URI del repository Amazon ECR
Asia Pacifico (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pacifico (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pacifico (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pacifico (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Medio Oriente (Bahrein)	558608220178.dkr.ecr.me-south-1.amazonaws.com
	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milano)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (Spagna)	455263428931.dkr.ecr.eu-south-2.amazonaws.com

Regione AWS	URI del repository Amazon ECR
	<code>531047660167.dkr.ecr.eu-south-2.amazonaws.com</code>
Africa (Città del Capo)	<code>877085696533.dkr.ecr.af-south-1.amazonaws.com</code>
	<code>379032919888.dkr.ecr.af-south-1.amazonaws.com</code>
Asia Pacifico (Melbourne)	<code>491585149902.dkr.ecr.ap-southeast-4.amazonaws.com</code>
	<code>750462861327.dkr.ecr.ap-southeast-4.amazonaws.com</code>
Israele (Tel Aviv)	<code>066635153087.dkr.ecr.il-central-1.amazonaws.com</code>
	<code>292660727137.dkr.ecr.il-central-1.amazonaws.com</code>
Asia Pacifico (Malesia)	<code>151610086707.dkr.ecr.ap-southeast-5.amazonaws.com</code>
Asia Pacifico (Thailandia)	<code>121268973566.dkr.ecr.ap-southeast-7.amazonaws.com</code>
Messico (centrale)	<code>730335286997.dkr.ecr.mx-central-1.amazonaws.com</code>
Asia Pacifico (Taipei)	<code>533267051163.dkr.ecr.ap-east-2.amazonaws.com</code>

Repository ECR per l'agente EKS versione 1.8.1 () **eks.build.1**

Questa sezione fornisce il repository Amazon ECR per l'agente Amazon EKS versione 1.8.1 (v1.8.1-eks-build.1). Se utilizzi la v1.8.1-eks-build.1, ti consigliamo di passare alla versione dell'agente

predefinita, che di solito è la versione più recente dell'agente. GuardDuty A tale scopo, identifica l'agente più recente da [Versioni agenti rilasciate per le risorse Amazon EKS](#), quindi esegui i passaggi indicati di seguito. [Aggiornamento manuale dell'agente di sicurezza per le risorse Amazon EKS](#)

La tabella seguente mostra il repository Amazon ECR URIs in cui è ospitata la versione dell'agente di GuardDuty sicurezza per 1.8.1-eks-build.1 Amazon EKS.

Regione AWS	URI del repository Amazon ECR
Stati Uniti occidentali (Oregon)	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europa (Parigi)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia Pacifico (Mumbai)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pacifico (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canada (Centrale)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Medio Oriente (Emirati Arabi Uniti)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (Londra)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
Stati Uniti occidentali (California settentrionale)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Stati Uniti orientali (Virginia settentrionale)	031903291036.dkr.ecr.us-east-1.amazonaws.com
Stati Uniti orientali (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com

Regione AWS	URI del repository Amazon ECR
Europa (Irlanda)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Sud America (San Paolo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stoccolma)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Francoforte)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zurigo)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia Pacifico (Singapore)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pacifico (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pacifico (Giacarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pacifico (Tokyo)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pacifico (Seoul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pacifico (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pacifico (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Medio Oriente (Bahrein)	541829937850.dkr.ecr.me-south-1.amazonaws.com

Regione AWS	URI del repository Amazon ECR
Europa (Milano)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (Spagna)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Africa (Città del Capo)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia Pacifico (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israele (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repository ECR per GuardDuty agente su (solo AWS Fargate Amazon ECS)

Come prerequisito per utilizzare Runtime Monitoring for Amazon ECS-Fargate, è necessario.

[Prerequisiti per l'accesso all'immagine del contenitore](#) L'immagine del contenitore sidecar dell' GuardDuty agente è archiviata in Amazon ECR, con i relativi livelli di immagine archiviati in Amazon S3. Per ulteriori informazioni, consulta [Come funziona il monitoraggio del runtime con Fargate \(solo Amazon ECS\)](#).

La tabella seguente mostra i repository Amazon ECR che ospitano l' GuardDuty agente per (solo AWS Fargate Amazon ECS) per ciascuno di essi. Regione AWS

Regione AWS	URI del repository Amazon ECR
Stati Uniti occidentali (Oregon)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guard-duty-agent-fargate

Regione AWS	URI del repository Amazon ECR
Europa (Parigi)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pacifico (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pacifico (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guard-duty-agent-fargate
Canada (Centrale)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Medio Oriente (Emirati Arabi Uniti)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Europa (Londra)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guard-duty-agent-fargate
Stati Uniti occidentali (California settentrionale)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guard-duty-agent-fargate
Stati Uniti orientali (Virginia settentrionale)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guard-duty-agent-fargate
Stati Uniti orientali (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guard-duty-agent-fargate

Regione AWS	URI del repository Amazon ECR
Europa (Irlanda)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guard-duty-agent-fargate
Sud America (San Paolo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guard-duty-agent-fargate
Europa (Stoccolma)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guard-duty-agent-fargate
Europa (Francoforte)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Europa (Zurigo)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pacifico (Singapore)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pacifico (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pacifico (Giacarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pacifico (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guard-duty-agent-fargate

Regione AWS	URI del repository Amazon ECR
Asia Pacifico (Seoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente (Bahrein)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Milano)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Spagna)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
Africa (Città del Capo)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
Israele (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate

Regione AWS	URI del repository Amazon ECR
Asia Pacifico (Malesia)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Thailandia)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate
Canada occidentale (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate
Messico (centrale)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Taipei)	259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate

Due agenti di sicurezza sullo stesso host sottostante

Le istanze Amazon EC2 possono supportare diversi tipi di carichi di lavoro. Quando configuri un agente di sicurezza automatizzato su un'istanza Amazon EC2, la stessa istanza EC2 potrebbe avere un altro agente di sicurezza tramite EKS.

Panoramica di

Prendi in considerazione uno scenario in cui hai abilitato il monitoraggio del runtime. Ora puoi abilitare l'agente automatizzato per Amazon EKS tramite GuardDuty. Hai anche abilitato l'agente automatizzato per Amazon EC2. Può succedere che sullo stesso host sottostante vengano installati due agenti di sicurezza, uno per Amazon EKS e l'altro per Amazon EC2. Ciò potrebbe comportare l'esecuzione di due agenti di sicurezza all'interno dello stesso host, che raccolgono eventi di runtime e li inviano a GuardDuty, generando potenzialmente risultati duplicati.

Impatto

- Quando più di un security agent è in esecuzione sullo stesso host, il tuo account potrebbe avere il doppio delle esigenze di elaborazione della CPU e della memoria. Per informazioni sui limiti di CPU e memoria per ogni tipo di risorsa, consulta [Prerequisiti](#) per quella risorsa.
- GuardDuty ha progettato la funzionalità Runtime Monitoring in modo tale che, anche in caso di sovrapposizione di due security agent che raccolgono eventi di runtime dallo stesso host sottostante, all'account venga addebitato solo un flusso di eventi di runtime.

Come GuardDuty gestisce più agenti

GuardDuty rileva quando due security agent sono in esecuzione sullo stesso host e ne designa solo uno come agente di sicurezza che raccoglie attivamente gli eventi di runtime. Il secondo agente consumerà risorse di sistema minime in modo da prevenire qualsiasi impatto sulle prestazioni delle applicazioni.

GuardDuty considera i seguenti scenari:

- Quando un'istanza EC2 rientra nell'ambito degli agenti di sicurezza di Amazon EKS e Amazon EC2, l'agente di sicurezza EKS ha la priorità. Ciò si applica solo quando utilizzi il security agent v1.1.0 o successivo per Amazon EC2. Le versioni precedenti degli agenti continueranno a funzionare e a raccogliere eventi di runtime perché le versioni precedenti degli agenti non sono influenzate dalla prioritizzazione.
- Quando sia Amazon EKS che Amazon EC2 dispongono di agenti di sicurezza GuardDuty gestiti e l'istanza Amazon EC2 è gestita anche tramite SSM, entrambi gli agenti di sicurezza verranno installati a livello di host. Una volta installati gli agenti, GuardDuty decide quale agente di sicurezza continuerà a funzionare. Quando entrambi i security agent sono in esecuzione, alla fine solo uno di essi raccoglierà gli eventi di runtime.
- Quando i security agent associati sia a EC2 che a EKS vengono eseguiti contemporaneamente, GuardDuty potrebbero generare risultati duplicati solo durante il periodo di sovrapposizione.

Questo può accadere quando:

- Gli agenti di sicurezza per EC2 e EKS sono configurati tramite GuardDuty (automaticamente) o
- La tua risorsa Amazon EKS dispone di un agente di sicurezza automatizzato.

- Quando l'agente di sicurezza EKS è già in esecuzione, se lo distribuisce manualmente sullo stesso host sottostante e soddisfa tutti i prerequisiti, GuardDuty potrebbe non installare un secondo agente di sicurezza.

Monitoraggio del runtime EKS in GuardDuty

EKS Runtime Monitoring fornisce una copertura per il rilevamento delle minacce in fase di esecuzione per i nodi e i contenitori Amazon Elastic Kubernetes Service (Amazon EKS) all'interno del tuo ambiente. AWS EKS Runtime Monitoring utilizza un agente GuardDuty di sicurezza che aggiunge visibilità in fase di runtime ai singoli carichi di lavoro EKS, ad esempio l'accesso ai file, l'esecuzione dei processi e le connessioni di rete. L'agente GuardDuty di sicurezza aiuta a GuardDuty identificare contenitori specifici all'interno dei cluster EKS che sono potenzialmente compromessi. Può anche rilevare i tentativi di trasferire i privilegi da un singolo container all'host EC2 sottostante e all'ambiente più ampio. AWS

Grazie alla disponibilità di Runtime Monitoring, GuardDuty ha consolidato l'esperienza della console per EKS Runtime Monitoring nel Runtime Monitoring. GuardDuty non migrerà automaticamente le impostazioni di EKS Runtime Monitoring per tuo conto. Ciò richiede un'azione da parte tua. Se desideri continuare a utilizzare solo EKS Runtime Monitoring, puoi utilizzare APIs o AWS CLI per controllare e aggiornare lo stato di configurazione esistente per EKS Runtime Monitoring. Tuttavia, GuardDuty consiglia [Migrazione da EKS Runtime Monitoring a Runtime Monitoring](#) e utilizza Runtime Monitoring per monitorare i cluster Amazon EKS.

Argomenti

- [Configurazione di EKS Runtime Monitoring per ambienti con più account \(API\)](#)
- [Configurazione di EKS Runtime Monitoring per un account autonomo \(API\)](#)
- [Migrazione da EKS Runtime Monitoring a Runtime Monitoring](#)

Configurazione di EKS Runtime Monitoring per ambienti con più account (API)

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare EKS Runtime Monitoring per gli account membro e gestire la gestione degli GuardDuty agenti per i cluster EKS appartenenti agli account membri della rispettiva organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account

GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta [Gestione di più account](#).

Configurazione di EKS Runtime Monitoring per l'account amministratore delegato GuardDuty

Questa sezione fornisce i passaggi per configurare EKS Runtime Monitoring e gestire il GuardDuty security agent per i cluster EKS che appartengono all'account amministratore delegato GuardDuty.

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#), puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" :</pre>

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	<pre>[{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}]]]'</pre>

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -false. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci ec2:CreateTags con eks:TagResource . - Sostituisci ec2:DeleteTags con eks:UntagResource . - Sostituisci access-project con GuardDutyManaged - Sostituisci 123456789012 con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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>  Note Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare STATUS of

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	EKS_RUNTIME_MONITORING toENABLED; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}]]'</pre>

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -true. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . - Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . - Sostituisci <i>access-project</i> con GuardDutyManaged - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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> Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Imposta lo stato di <code>EKS_ADDON_MANAGEMENT</code> su <code>DISABLED</code>. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la <code>true</code> coppia <code>GuardDutyManaged</code> -. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. L'esempio seguente abilita <code>EKS_RUNTIME_MONITORING</code> e disabilita <code>EKS_ADDON_MANAGEMENT</code> : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre>

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestire l'agente di sicurezza manualmente	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectorsAPI. L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}]]'</pre> Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilitare automaticamente il monitoraggio del runtime EKS per tutti gli account membri

Questa sezione include i passaggi per abilitare EKS Runtime Monitoring e gestire l'agente di sicurezza per tutti gli account membri. Ciò include l'account GuardDuty amministratore delegato, gli account dei membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#), puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione updateMemberDetectors API utilizzando la tua. <i>detector ID</i> Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <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>  Note Puoi anche passare un elenco di account IDs separati da uno spazio.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code> . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDuty Managed -false. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . - Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . - Sostituisci <i>access-project</i> con <code>GuardDutyManaged</code> - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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> Note Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare STATUS of EKS_RUNTIME_MONITORING toENABLED; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <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>  Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts . Se si verifica qualsiasi

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	problema durante la modifica delle impostazioni del rilevatore e di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDuty Managed -true. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . • Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . • Sostituisci <i>access-project</i> con <code>GuardDutyManaged</code> • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <pre data-bbox="633 1228 1412 1396">"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. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su <code>EKS_RUNTIME_MONITORING</code> e lo stato su <code>ENABLED</code>. Imposta lo stato di <code>EKS_ADDON_MANAGEMENT</code> su <code>DISABLED</code>. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la <code>true</code> coppia <code>GuardDutyManaged</code> -.

Approccio preferito per gestire l'agente GuardDuty di sicurezza

Fasi

In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita 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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore e di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita EKS_ADDON_MANAGEMENT : <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": "ENABLED"}]}]'</pre> Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione del monitoraggio del runtime EKS per tutti gli account membri attivi esistenti

Questa sezione include i passaggi per abilitare EKS Runtime Monitoring e gestire l'agente di GuardDuty sicurezza per gli account dei membri attivi esistenti nell'organizzazione.

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#), puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione updateMemberDetectors API utilizzando la tua <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <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>  Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code> . Se si verifica qualsiasi problema

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza

Fasi

durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDuty Managed -false. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con <code>eks:TagResource</code> . - Sostituisci <i>ec2:DeleteTags</i> con <code>eks:UntagResource</code> . - Sostituisci <i>access-project</i> con <code>GuardDutyManaged</code> - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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.  Note Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare STATUS of EKS_RUNTIME_MONITORING toENABLED; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	Per abilitare selettivamente EKS Runtime Monitoring per i vostri account membri, eseguite l'operazione updateMemberDetectors API utilizzando le vostre. <i>detector ID</i> Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <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>  Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts . Se si verifica qualsiasi

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	problema durante la modifica delle impostazioni del rilevatore e di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDuty Managed -true. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con <i>eks:TagResource</i> . • Sostituisci <i>ec2:DeleteTags</i> con <i>eks:UntagResource</i> . • Sostituisci <i>access-project</i> con GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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. Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione updateMemberDetect API utilizzando la tua <i>detector ID</i> Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la true coppia GuardDutyManaged -.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza

Fasi

In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore e di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione updateMemberDetectors API utilizzando la tua <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita EKS_ADDON_MANAGEMENT : <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": "ENABLED"}] }]'</pre> Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilitare automaticamente il monitoraggio del runtime EKS per i nuovi membri

L'account GuardDuty amministratore delegato può abilitare automaticamente EKS Runtime Monitoring e scegliere un approccio per la gestione del GuardDuty security agent per i nuovi account che entrano a far parte dell'organizzazione.

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#), puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare selettivamente EKS Runtime Monitoring per i tuoi nuovi account, richiama l'operazione UpdateOrganizationConfiguration API utilizzando la tua <i>detector ID</i> Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le <code>detectorId</code> informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. <pre data-bbox="672 1560 1438 1787">aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre>

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code> . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -false. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . - Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . - Sostituisci <i>access-project</i> con GuardDutyManaged - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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>  Note Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare STATUS of

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	EKS_RUNTIME_MONITORING toENABLED; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Per abilitare selettivamente EKS Runtime Monitoring per i tuoi nuovi account, richiama l'operazione UpdateOrganizationConfiguration API utilizzando la tua <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le <code>detectorId</code> informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	<pre data-bbox="716 268 1507 573">aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code> . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -true. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . - Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . - Sostituisci <i>access-project</i> con GuardDutyManaged - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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> Per abilitare selettivamente EKS Runtime Monitoring per i tuoi nuovi account, richiama l'operazione UpdateOrganizationConfigurationAPI utilizzando la tua <i>detector ID</i>

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Imposta lo stato di <code>EKS_ADDON_MANAGEMENT</code> su <code>DISABLED</code>. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la <code>true</code> coppia <code>GuardDutyManaged</code>. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente viene abilitato <code>EKS_RUNTIME_MONITORING</code> e disabilitato <code>EKS_ADDON_MANAGEMENT</code> per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le <code>detectorId</code> informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. <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> Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code>. Se si

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestire l'agente di sicurezza manualmente	1. Per abilitare selettivamente EKS Runtime Monitoring per i tuoi nuovi account, richiama l'operazione UpdateOrganizationConfiguration API utilizzando la tua <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente viene abilitato EKS_RUNTIME_MONITORING e disabilitato EKS_ADDON_MANAGEMENT per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. <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> Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts . Se si

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema. 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilitare il monitoraggio del runtime EKS per singoli account membri attivi

Questa sezione include i passaggi per configurare EKS Runtime Monitoring e gestire il security agent per i singoli account dei membri attivi.

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#), puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione updateMemberDetectors API utilizzando la tua <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza

Fasi

console.aws.amazon.com/guardduty/console o esegui l'[ListDetectorsAPI](#).

Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che 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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -false. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . • Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . • Sostituisci <i>access-project</i> con GuardDutyManaged • Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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>

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	3.  Note Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare STATUS of EKS_RUNTIME_MONITORING to ENABLED; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Per abilitare selettivamente EKS Runtime Monitoring per i vostri account membri, eseguite l'operazione updateMemberDetectors API utilizzando le vostre <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature</pre>

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	<pre>s ' [{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }] '</pre>  Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code> . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -true. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . - Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . - Sostituisci <i>access-project</i> con GuardDuty Managed - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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> Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza

Fasi

[updateMemberDetectors](#) API utilizzando la tua *detector ID*.

Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED.

GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la `true` coppia GuardDutyManaged -.

In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita EKS_ADDON_MANAGEMENT :

```
aws guardduty update-member-detectors --  
detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --feature  
s '[{"Name" : "EKS_RUNTIME_MONITORING",  
  "Status" : "ENABLED", "AdditionalConfigu  
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",  
  "Status" : "DISABLED"}] ]'
```

Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di <code>UnprocessedAccounts</code> . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	Per abilitare selettivamente EKS Runtime Monitoring per i tuoi account membri, esegui l'operazione updateMemberDetectors API utilizzando la tua <i>detector ID</i>. Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita EKS_ADDON_MANAGEMENT : <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" : "ENABLED"}] }]'</pre> Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione di EKS Runtime Monitoring per un account autonomo (API)

A un account indipendente spetta la decisione di abilitare o disabilitare un piano di protezione all'interno di uno specifico Account AWS account. Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Configurazione di EKS Runtime Monitoring per ambienti con più account \(API\)](#).

Dopo aver abilitato il Runtime Monitoring, assicurati GuardDuty di installare Security Agent tramite la configurazione automatica o la distribuzione manuale. Come parte del completamento di tutti i passaggi elencati nella procedura seguente, assicuratevi di installare il security agent.

In base a [Approcci per gestire gli agenti GuardDuty di sicurezza nei cluster Amazon EKS](#), puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto <code>features</code> su <code>EKS_RUNTIME_MONITORING</code> e lo stato su <code>ENABLED</code>. Imposta lo stato di <code>EKS_ADDON_MANAGEMENT</code> su <code>ENABLED</code>. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia <code>EKS_RUNTIME_MONITORING</code> che <code>EKS_ADDON_MANAGEMENT</code> : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "Addition</pre>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	<pre>alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " <i>ENABLED</i>"}] }]'</pre>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -false. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . - Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . - Sostituisci <i>access-project</i> con GuardDutyManaged - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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>  Note Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare STATUS of

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	EKS_RUNTIME_MONITORING toENABLED; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su ENABLED. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia EKS_RUNTIME_MONITORING che EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}]]'</pre>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è GuardDutyManaged -true. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: - Sostituisci <i>ec2:CreateTags</i> con eks:TagResource . - Sostituisci <i>ec2:DeleteTags</i> con eks:UntagResource . - Sostituisci <i>access-project</i> con GuardDutyManaged - Sostituisci <i>123456789012</i> con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn : <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> Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Imposta lo stato di <code>EKS_ADDON_MANAGEMENT</code> su <code>DISABLED</code>. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la <code>true</code> coppia <code>GuardDutyManaged</code>. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice <code>detectorId</code> relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectors API. L'esempio seguente abilita <code>EKS_RUNTIME_MONITORING</code> e disabilita <code>EKS_ADDON_MANAGEMENT</code> : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre>

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto features su EKS_RUNTIME_MONITORING e lo stato su ENABLED. Imposta lo stato di EKS_ADDON_MANAGEMENT su DISABLED. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console o esegui l'ListDetectorsAPI. L'esempio seguente abilita EKS_RUNTIME_MONITORING e disabilita EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre> Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Migrazione da EKS Runtime Monitoring a Runtime Monitoring

Con il lancio di GuardDuty Runtime Monitoring, la copertura per il rilevamento delle minacce è stata estesa ai contenitori Amazon ECS e alle istanze Amazon EC2. L'esperienza di EKS Runtime Monitoring è stata ora consolidata nel Runtime Monitoring. Puoi abilitare il monitoraggio del runtime

e gestire singoli agenti di GuardDuty sicurezza per ogni tipo di risorsa (istanza Amazon EC2, cluster Amazon ECS e cluster Amazon EKS) per cui desideri monitorare il comportamento di runtime.

GuardDuty ha consolidato l'esperienza della console per EKS Runtime Monitoring in Runtime Monitoring. GuardDuty consiglia [Verifica dello stato della configurazione di EKS Runtime Monitoring](#) e [Migrazione da EKS Runtime Monitoring a Runtime Monitoring](#).

Come parte della migrazione al Runtime Monitoring, assicurati di [Disabilita il monitoraggio del runtime EKS](#). Questo è importante perché se in seguito scegliete di disabilitare il Runtime Monitoring e non disattivate EKS Runtime Monitoring, continuerete a sostenere costi di utilizzo per EKS Runtime Monitoring.

Per migrare da EKS Runtime Monitoring a Runtime Monitoring

1. La GuardDuty console supporta EKS Runtime Monitoring come parte del Runtime Monitoring.

Puoi iniziare a utilizzare Runtime Monitoring in base [Verifica dello stato della configurazione di EKS Runtime Monitoring](#) alla tua organizzazione e ai tuoi account.

Assicuratevi di non disabilitare EKS Runtime Monitoring prima di abilitare Runtime Monitoring. Se disabiliti EKS Runtime Monitoring, verrà disabilitata anche la gestione dei componenti aggiuntivi di Amazon EKS. Continua con i seguenti passaggi nell'ordine indicato.

2. Assicurati di soddisfare tutti i [Prerequisiti per abilitare il monitoraggio del runtime](#).
3. Abilita il monitoraggio del runtime replicando le stesse impostazioni di configurazione dell'organizzazione per il monitoraggio del runtime utilizzate per EKS Runtime Monitoring. Per ulteriori informazioni, consulta [Abilitazione del monitoraggio del runtime](#).

- Se disponi di un account autonomo, devi abilitare il Runtime Monitoring.

Se il GuardDuty security agent è già distribuito, le impostazioni corrispondenti vengono replicate automaticamente e non è necessario configurarle nuovamente.

- Se hai un'organizzazione con impostazioni di attivazione automatica, assicurati di replicare le stesse impostazioni di attivazione automatica per Runtime Monitoring.
- Se hai un'organizzazione con impostazioni configurate singolarmente per gli account dei membri attivi esistenti, assicurati di abilitare il Runtime Monitoring e di configurare il GuardDuty security agent per questi membri singolarmente.

4. Dopo esserti assicurato che le impostazioni del Runtime Monitoring e del GuardDuty security agent siano corrette, [disabilita EKS Runtime Monitoring](#) utilizzando l'API o il AWS CLI comando.

5. (Facoltativo) se desideri pulire qualsiasi risorsa associata al GuardDuty security agent, consulta [Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring](#).

Se desideri continuare a utilizzare EKS Runtime Monitoring senza abilitare il Runtime Monitoring, consulta [Monitoraggio del runtime EKS in GuardDuty](#). In base al tuo caso d'uso, scegli i passaggi per configurare EKS Runtime Monitoring per un account autonomo o per più account membri.

Verifica dello stato della configurazione di EKS Runtime Monit

Utilizza i seguenti AWS CLI comandi APIs per verificare lo stato di configurazione esistente di EKS Runtime Monitoring.

Per verificare lo stato di configurazione di EKS Runtime Monitoring esistente nel tuo account

- Esegui [GetDetector](#) per controllare lo stato di configurazione del tuo account.
- In alternativa, puoi eseguire il seguente comando utilizzando AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

Assicurati di sostituire l'ID del rilevatore della tua regione Account AWS e di quella attuale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Per verificare lo stato di configurazione di EKS Runtime Monitoring esistente per la vostra organizzazione (solo come account GuardDuty amministratore delegato)

- Esegui [DescribeOrganizationConfiguration](#) per verificare lo stato di configurazione della tua organizzazione.

In alternativa, puoi eseguire il seguente comando usando AWS CLI:

```
aws guardduty describe-organization-configuration --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Assicurati di sostituire l'ID del rilevatore con l'ID del tuo account GuardDuty amministratore delegato e la regione con la regione corrente. Per trovare il codice `detectorId` relativo

al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'API. [ListDetectors](#)

Disattivazione di EKS Runtime Monitoring dopo la migrazione a Runtime Monitoring

Dopo esserti assicurato che le impostazioni esistenti per il tuo account o la tua organizzazione siano state replicate in Runtime Monitoring, puoi disabilitare EKS Runtime Monitoring.

Per disabilitare EKS Runtime Monitoring

- Per disabilitare EKS Runtime Monitoring nel proprio account

Esegui l'[UpdateDetector](#) API con la tua area regionale *detector-id*.

In alternativa, puoi usare il seguente AWS CLI comando. Sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con il tuo regionale *detector-id*.

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

- Per disabilitare EKS Runtime Monitoring per gli account dei membri dell'organizzazione

Esegui l'[UpdateMemberDetectors](#) API con l'account regionale *detector-id* dell' GuardDuty amministratore delegato dell'organizzazione.

In alternativa, puoi usare il seguente AWS CLI comando. Sostituisci *12abc34d567e8fa901bc2d34e56789f0* con l'account regionale *detector-id* dell' GuardDuty amministratore delegato dell'organizzazione e *111122223333* con l' Account AWS ID dell'account membro per il quale desideri disabilitare questa funzione.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",  
"Status" : "DISABLED"}]'
```

- Per aggiornare EKS Runtime Monitoring, abilita automaticamente le impostazioni per la tua organizzazione

Eseguite il passaggio seguente solo se avete configurato le impostazioni di attivazione automatica di EKS Runtime Monitoring per gli account nuovi (NEW) o per tutti (ALL) i membri dell'organizzazione. Se l'hai già configurato come NONE, puoi saltare questo passaggio.

 Note

L'impostazione della configurazione di attivazione automatica di EKS Runtime Monitoring NONE significa che EKS Runtime Monitoring non verrà abilitato automaticamente per nessun account membro esistente o quando un nuovo account membro si unisce all'organizzazione.

Esegui l'[UpdateOrganizationConfiguration](#) API con l'account regionale *detector-id* dell'GuardDuty amministratore delegato dell'organizzazione.

In alternativa, puoi usare il seguente AWS CLI comando. Sostituisci *12abc34d567e8fa901bc2d34e56789f0* con l'account regionale *detector-id* dell'GuardDuty amministratore delegato dell'organizzazione. *EXISTING_VALUE* Sostituiscila con la tua configurazione attuale per l'attivazione automatica GuardDuty.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

GuardDuty versioni di rilascio di Security Agent

GuardDuty rilascia di tanto in tanto una versione aggiornata dell'agente. When GuardDuty gestisce l'agente automaticamente, GuardDuty è progettato per aggiornare l'agente per tuo conto. Quando gestisci l'agente manualmente, sei responsabile dell'aggiornamento della versione dell'agente per i tuoi tipi di risorse: istanze Amazon EC2, cluster Amazon ECS e cluster Amazon EKS.

Le seguenti sezioni forniscono le versioni di rilascio GuardDuty degli agenti di sicurezza e le relative note di rilascio per tutti i tipi di risorse supportati.

Argomenti

- [GuardDuty versioni degli agenti di sicurezza per le istanze Amazon EC2](#)
- [GuardDuty versioni degli agenti di sicurezza per AWS Fargate \(solo Amazon ECS\)](#)
- [GuardDuty versioni degli agenti di sicurezza per le risorse Amazon EKS](#)
- [Risorse aggiuntive: fasi successive](#)

GuardDuty versioni degli agenti di sicurezza per le istanze Amazon EC2

La tabella seguente mostra la cronologia delle versioni di rilascio del GuardDuty Security Agent per Amazon EC2.

Versione del distributore SSM	Versione agente	Note di rilascio	Data di disponibilità
v1.9.2	v1.9.2	Aggiunto il supporto per Kernel 6.15, 6.16, 6.17, 6.18. È stato aggiunto il supporto per Alma Linux 9, Alma Linux 10 e SUSE Linux Enterprise Server 16. Per un elenco di tutte le distribuzioni di sistemi operativi verificate per le risorse Amazon EC2, consulta. Convalida i requisiti architetturici	24 febbraio 2026
v1.9.1	v1.9.1	Ottimizzazione generale delle prestazioni e aggiornamenti delle funzionalità di sicurezza.	10 novembre 2025
v1.9.0	v1.9.0	Ottimizzazione e miglioramenti generali delle prestazioni.	23 ottobre 2025

Versione del distributore SSM	Versione agente	Note di rilascio	Data di disponibilità
v1.8.0	v1.8.0	Ottimizzazione e miglioramenti generali delle prestazioni.	12 agosto 2025
v1.7.2	versione 1.7.1	Supporto migliorato per l'installazione di agenti locali per le distribuzioni Linux basate su RPM.	23 luglio 2025
versione 1.7.1	1.7.1	Aggiunto il supporto per Fedora 40 e Fedora 41. Per un elenco di tutte le distribuzioni di sistemi operativi verificate per le risorse Amazon EC2, consulta. Convalida i requisiti architetturali Ottimizzazione e miglioramenti generali delle prestazioni.	03 giugno 2025

Versione del distributore SSM	Versione agente	Note di rilascio	Data di disponibilità
v1.7.0	v1.7.0	È stato aggiunto il supporto per le versioni 8.9 e 9.3 di Oracle Linux e la versione 9.5 di Rocky Linux. Per un elenco di tutte le distribuzioni di sistemi operativi verificate per le risorse Amazon EC2, consulta. Convalida i requisiti architetturici Risoluzione migliorata degli ID dei container. Ottimizzazione e miglioramenti generali delle prestazioni.	3 aprile 2025
v1.6.0	v1.6.0	Ottimizzazione e miglioramenti generali delle prestazioni.	6 febbraio 2025

Versione del distributore SSM	Versione agente	Note di rilascio	Data di disponibilità
v1.5.0	v1.5.0	È stato aggiunto il supporto per CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 e Ubuntu 24.04. Support per le istanze ARM per i . . . / MetadataDNSRebind risultati. Ottimizzazione e miglioramenti generali delle prestazioni.	20 novembre 2024
v1.3.1	v1.3.1	Support per resolver DNS personalizzati.	12 settembre 2024
v1.3.0	v1.3.0	Ottimizzazione e miglioramenti generali delle prestazioni. Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuro GuardDuty Tipi di risultati del monitoraggio del runtime.	19 agosto 2024

Versione del distributore SSM	Versione agente	Note di rilascio	Data di disponibilità
v1.2.0	v1.2.0	Supporta le distribuzioni del sistema operativo Ubuntu 20.04, Ubuntu 22.04, Debian 11 e Debian 12. Supporta kernel 6.5 e 6.8. Ottimizzazione e miglioramenti generali delle prestazioni.	13 giugno 2024
v1.1.0	v1.1.0	Supporta la configurazione GuardDuty automatizzata degli agenti in Runtime Monitoring per le istanze Amazon EC2. Supporta nuovi segnali e risultati di sicurezza rilasciati con l'annuncio della disponibilità generale di Runtime Monitoring per le istanze EC2. Ottimizzazione e miglioramenti generali delle prestazioni.	26 marzo 2024

Versione del distributore SSM	Versione agente	Note di rilascio	Data di disponibilità
v1.0.2	v1.0.2	Supporta la versione più recente di Amazon ECS. AMIs	2 febbraio 2024
v1.0.1	v1.0.1	Le versioni degli agenti rilasciate prima della v1.0.2 sono incompatibili con Amazon ECS AMIs lanciato dopo il 31 gennaio 2024. Ottimizzazione e miglioramenti generali delle prestazioni.	23 gennaio 2024
v1.0.0	v1.0.0	Versione iniziale dell'installazione RPM. Le versioni degli agenti rilasciate prima della v1.0.2 sono incompatibili con Amazon ECS AMIs lanciato dopo il 31 gennaio 2024.	26 novembre 2023

GuardDuty versioni degli agenti di sicurezza per AWS Fargate (solo Amazon ECS)

La tabella seguente mostra la cronologia delle versioni di rilascio del GuardDuty Security Agent per Fargate (solo Amazon ECS).

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.9.0	x86_64 (): AMD64 sha256:fd9acaa2326f180f0ed0c5a25d8ffa2d0498a6e900c34c68d4e973ea7fb26a8 Gravitone (): ARM64 sha256:0b04f8c28956684e752677bfd83dbc45afc8a43f7791fa44667b8078ba48a295	Ottimizzazione generale delle prestazioni e miglioramenti della sicurezza.	28 ottobre 2025
v1.8.0	x86_64 (): AMD64 sha256:4425417f39e38b24c1be428bacad1dad53e0645530dcf4422436353bfe358e3a Gravitone (): ARM64 sha256:af069418fd6825846f8	Ottimizzazione e miglioramenti generali delle prestazioni.	12 agosto 2025

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
	f575c4990 6a67c8a44 6d12d9ed0 d21ab95bd 0d05497b		
v1.7.0	x86_64 (): AMD64 sha256:bf 9197abdf8 53607e5fa 392b4f97c cdd6ca56d d179be3ce 8849e552d 96582ac8 Gravitone (): ARM64 sha256:56 c8683c948 bcd82c0db cebf75520 4365ac728 5994693c1 1717bd45f 86e279c2	Risoluzione dell'ID del contenitore migliorata. Ottimizzazione e miglioramenti generali delle prestazioni.	04 aprile 2025

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.6.0	x86_64 (): AMD64 sha256:c8 dea71d372 bc47b2f23 6f7a091b9 a9b06bc81 93c1cfe4c 9346eb50f 89258897 Gravitone (): ARM64 sha256:f4 032a566b9 0537646c2 a987bef42 eca1b4980 78ccc58a8 48603f877 971a8dbe	Ottimizzazione e miglioramenti generali delle prestazioni.	6 febbraio 2025

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.5.0	x86_64 (): AMD64 sha256:5e6fdc41f9eb748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54 Gravitone (): ARM64 sha256:d56801ff6864d6014740103b70b1c38431851358d182613bede20fe21090e734	Support per le attività ARM relative . . . / MetadataDNSRebind ai risultati. Ottimizzazione e miglioramenti generali delle prestazioni.	14 novembre 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.4.1	x86_64 (): AMD64 sha256:ef36a11151ec2d3d7db22273bfb954750dee76f0ac7bec37a7ba7e74c3de1c78 Gravitone (): ARM64 sha256:a8844544a59d6b4cba98f8e528b513ac2d97432f208e3ad497cc16b331aa9faa	Indurimento dell'immagine del contenitore. Ottimizzazione e miglioramenti generali delle prestazioni.	24 ottobre 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.3.1	x86_64 (): AMD64 sha256:a6 e2307d796 e2875907b c4c1c6962 2c906f319 2ddc42ef2 7b99e0a8f 0979f3e0 Gravitone (): ARM64 sha256:ad 1b6539d80 6edb504f1 7e6bcfb8b 4026c5e82 2300afc31 c0d23c6a0 8f9b99e9	Support per resolver DNS personalizzati.	11 settembre 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.3.0	x86_64 (): AMD64 sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831 Gravitone (): ARM64 sha256:ff81a755d46681e409f55a95beeda e9ebbcf5336e1c0b1e6348af7c6518bdbb1	Ottimizzazione e miglioramenti generali delle prestazioni. Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuro GuardDuty GuardDuty Tipi di risultati del monitoraggio del runtime.	9 agosto 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.2.0	x86_64 (): AMD64 sha256:1d bad20ac2d c66d52d00 bb28dde42 81fe0d3c5 f261b1649 b247c2369 d9e26b93 Gravitone (): ARM64 sha256:91 930f8446f 5f95b93b8 ccb187739 92affa401 eb3f42da8 9d68077a5 6bafa6cd	Ottimizzazione e miglioramenti generali delle prestazioni.	31 maggio 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.1.0	x86_64 (): AMD64 sha256:83 ce3cf2ef8 5a349ed17 97a8cf30a 008ac5d8c 9f673f283 5823957e9 dcf71657 Gravitone (): ARM64 sha256:0d 4b61648d7 bdeab8ab8 d94684f80 5498927c7 d437d3182 04dccccfe8 c9383dc7	Supporta nuovi segnali e risultati di sicurezza. Ottimizzazione e miglioramenti generali delle prestazioni.	01 maggio 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.0.1	x86_64 (): AMD64 sha256:9f8cd438fb66f62d09bf c641286439f7ed5177988a314a6021ef4ff880642e68 Gravitone (): ARM64 sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	Ottimizzazione e miglioramenti generali delle prestazioni.	26 gennaio 2024

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità
v1.0.0	x86_64 (): AMD64 sha256:35 9b8b014e5 076c625da a1056090e 522631587 a7afa3b2e 055edda6b d1141017 Gravitone (): ARM64 sha256:b9 438690fa8 a86067180 a11658bec 0f4f838ae 3fbd225d0 4b9306250 648b3984	Versione iniziale di GuardDuty Security Agent per AWS Fargate (solo Amazon ECS).	26 novembre 2023

GuardDuty versioni degli agenti di sicurezza per le risorse Amazon EKS

GuardDuty rilascia di tanto in tanto una versione aggiornata dell'agente. Quando GuardDuty gestisce l'agente automaticamente, è progettato per gestire gli aggiornamenti dell'agente per conto dell'utente. Quando gestisci l'agente manualmente, sei responsabile dell'aggiornamento della versione dell'agente per i tuoi cluster Amazon EKS.

Prima di aggiornare l'agente a una versione specifica, aggiungi il registro delle immagini GuardDuty al tuo controller `allowed-container-registries` di ammissione. Per ulteriori informazioni, consulta [Agente di hosting del repository Amazon ECR GuardDuty](#).

La tabella seguente mostra la cronologia delle versioni di rilascio dell' [GuardDuty agente aggiuntivo Amazon EKS](#).

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.12.1	x86_64 (): AMD64 sha256:f29a597745e5acff48809bebac7d8091bbc38229453dd26710c549b817362491 Gravitone (): ARM64 sha256:089cebd7e891177e107a099c9a4e362d9d74b5362cd374b448a16078040f6c6	Ottimizzazione generale delle prestazioni e aggiornamenti delle funzionalità di sicurezza.	17 novembre 2025	–
v1.11.0	x86_64 (): AMD64 sha256:7c398fd50de5fe493c361aa7fe191e094ddfa000c65b449a9ed6a5cd53610e7	È stato aggiunto il supporto per le distribuzioni OS Fedora 40 e Fedora 41. Per ulteriori informazioni, vedere Convalida dei requisiti relativi	29 agosto 2025	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
	Gravitone (): ARM64 sha256:98 a547b47d4 770f45e75 eb9730c80 7d9265722 ca2f391e0 aa5cb19e4 87ab455f	all'architettura (per EKS). Ottimizzazione generale delle prestazioni e miglioramenti della sicurezza.		
v1.10.0	x86_64 (): AMD64 sha256:6d cbe5b055e 1ef0af903 071ede0b0 8f755ad5b 7e9774a67 df5399efd aa1f3d7d Gravitone (): ARM64 sha256:f0 536882268 9610a4bab 543abf93d 3e070b1b5 59e62a2e6 7d82dfa98 37600f72	Risoluzione dell'ID del contenitore migliorata. Ottimizzazione e miglioramenti generali delle prestazioni.	04 aprile 2025	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.9.0	x86_64 (): AMD64 sha256:51 c5789ef65 70f9bec87 9ac48a8f4 769718cbc 31e454300 32569917e 219af63f Gravitone (): ARM64 sha256:9c 2f74e7ea0 827b7e422 ae4c91fff c6c2bc41a 1cdb96c71 91d05259d 337154e1	Ottimizzazione e miglioramenti generali delle prestazioni.	02 marzo 2025	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.8.1	x86_64 (): AMD64 sha256:f2ce8cf89db e17e3388c ecb350535 44dadf21a f7770545f 8d4b50384 076aff47 Gravitone (): ARM64 sha256:30f586e4b69 4e704bcaf adfa9081a b0aef3cf bcde39743 a0f1e24f7 7d79627f	È stato aggiunto il supporto per CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 e Ubuntu 24.04. Support per la .../Metad ataDNSReb ind ricerca di istanze ARM. Ottimizzazione e miglioramenti generali delle prestazioni.	23 novembre 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
versione 1.7.1	x86_64 (): AMD64 sha256:b8b86b5d0872c8b67fecf64ec3d172666360545435a1752447d510951a7fd749 Gravitone (): ARM64 sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9	Ottimizzazione e miglioramenti generali delle prestazioni. Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuro GuardDuty Tipi di risultati del monitoraggio del runtime . Support per resolver DNS personalizzati.	13 settembre 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.7.0	x86_64 (): AMD64 sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffc7e68554a423d610cea8c7e8f2185ec Gravitone (): ARM64 sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a	Ottimizzazione e miglioramenti generali delle prestazioni. Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuro GuardDuty Tipi di risultati del monitoraggio del runtime .	17 agosto 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.6.1	x86_64 (): AMD64 sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bd07c3ab1 Gravitone (): ARM64 sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afc43a8902b4d71019	Ottimizzazione e miglioramenti generali delle prestazioni.	14 maggio 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.6.0	x86_64 (): AMD64 sha256:7d abcbec30d 8b0536767 52fbc19e8 9f77272d9 a6a53cc93 731f58721 80ef9010 Gravitone (): ARM64 sha256:97 10f53afcc df4f22b26 5a1a6fc27 f1469403a f1f7d5d08 c4869a726 9cdd2650	• Supporta la configurazione GuardDuty automatica degli agenti per le risorse EKS/EC2. • Supporta i nuovi segnali e risultati di sicurezza. Per ulteriori informazioni, consultare Tipi di eventi di runtime raccolti che GuardDuty utilizzano e GuardDuty Tipi di risultati del monitoraggio del runtime. • Ottimizzazione e miglioramenti generali delle prestazioni.	29 aprile 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.5.0	x86_64 (): AMD64 sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Gravitone (): ARM64 sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	• Ottimizzazione e miglioramenti generali delle prestazioni. • Miglioramenti della sicurezza, inclusi nuovi tipi di eventi in. Tipi di eventi di runtime raccolti • Miglioramenti delle prestazioni relativi all'utilizzo della CPU.	07 marzo 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.4.1	x86_64 (): AMD64 sha256:66 d49192776 3742660fa a87cc2c39 bb97b7873 039157ae8 b90bc999c b73d0b9c Gravitone (): ARM64 sha256:53 7a330b2dd 82357024f b6daeb876 1034b7def d43b10dff e0792c9e6 d0778b40	Ottimizzazione e miglioramenti generali delle prestazioni.	16 gennaio 2024	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.4.0	x86_64 (): AMD64 sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f Gravitone (): ARM64 sha256:0c650aeafee b5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e	Il punto di montaggio Manifest supporta una migliore raccolta dei dati AppArmor configurazione in manifest Raccogli l'argomento della riga di comando Ottimizzazione e miglioramenti generali delle prestazioni	21 dicembre 2023	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.3.1	x86_64 (): AMD64 sha256:55 578fcb7b7 3097ade5c 8404390ef 16cf76a7b 568490aba ae01ac759 92b3ea29 Gravitone (): ARM64 sha256:e3 ce8d66ac2 121f8d476 eb58f8bc5 0ab513366 47615eb7c f514c2142 1cb818fd	Patch di sicurezza e aggiornamenti importanti.	23 ottobre 2023	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.3.0	x86_64 (): AMD64 sha256:6d ace2337df bb7609811 be89fb4b2 3ae0b865f 1027ad78f be69530bf bd46c694 Gravitone (): ARM64 sha256:49 28a7c6ef4 0e77c8ec9 5841323bb 9a110db31 f12c0ee7a b965e08b4 3efd01bb	Supporta la piattaforma Ubuntu Supporta la versione 1.28 di Kubernetes Miglioramenti generali delle prestazioni e miglioramento della stabilità.	5 ottobre 2023	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.2.0	x86_64 (): AMD64 sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3 Gravitone (): ARM64 sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa	Oltre alle istanze AMD64 basate, la versione 1.2.0 ora supporta anche le istanze basate. ARM64 È stato aggiunto e verificato il supporto per Bottlerocket Supporta la versione 1.27 di Kubernetes Miglioramenti generali delle prestazioni e miglioramenti della stabilità.	16 giugno 2023	–

Versione agente	Immagine del contenitore	Note di rilascio	Data di disponibilità	Fine del supporto standard ¹
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	Oltre a Versioni di Kubernetes supportate dal security agent GuardDuty , questa versione dell'agente supporta anche la versione 1.26 di Kubernetes. Miglioramenti generali delle prestazioni e miglioramenti della stabilità.	2 maggio 2023	14 maggio 2024
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Versione iniziale dell'agente (componente aggiuntivo di Amazon EKS).	30 marzo 2023	14 maggio 2024

¹ Per informazioni sull'aggiornamento della versione corrente dell'agente che si avvicina alla fine del supporto standard, consulta. [Aggiornamento manuale dell'agente di sicurezza per le risorse Amazon EKS](#)

Risorse aggiuntive: fasi successive

Per ulteriori informazioni sui passaggi successivi, consulta i seguenti argomenti:

- [Prerequisiti per abilitare il monitoraggio del runtime](#)- Con le nuove versioni degli agenti, potrebbe esserci un aggiornamento alla sezione dei prerequisiti. Verifica e convalida che le tue risorse soddisfino i prerequisiti più recenti.
- [Gestione degli agenti GuardDuty di sicurezza](#)- Quando gestisci l'agente manualmente, sei responsabile della gestione degli aggiornamenti della versione dell'agente in esecuzione sulle tue risorse. In base al tipo di risorsa (Amazon EKS o Amazon EC2-Amazon ECS), esegui i passaggi per aggiornare il security agent. Assicurati inoltre di convalidare la configurazione dell'[endpoint VPC](#).
- [Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi](#)- Dopo aver aggiornato il security agent, puoi valutare la copertura in fase di runtime della tua risorsa. In caso di problemi di copertura, utilizza i passaggi di risoluzione dei problemi associati.

Disattivazione, disinstallazione e pulizia delle risorse in Runtime Monitoring

Questa sezione si applica Account AWS se si sceglie di disabilitare il Runtime Monitoring o solo la configurazione GuardDuty automatica dell'agente per un tipo di risorsa.

Disabilitazione della configurazione GuardDuty automatica degli agenti

GuardDuty non rimuove il security agent distribuito sulla tua risorsa. Tuttavia, GuardDuty smetterà di gestire gli aggiornamenti del security agent.

GuardDuty continua a ricevere gli eventi di runtime dal tipo di risorsa in uso. Per evitare un impatto sulle statistiche di utilizzo, assicurati di rimuovere il GuardDuty security agent dalla tua risorsa.

Indipendentemente dal fatto che un Account AWS utente utilizzi o meno un endpoint VPC condiviso, GuardDuty non elimina l'endpoint VPC. Se necessario, dovrai eliminare l'endpoint VPC manualmente.

Disabilitazione del monitoraggio del runtime e del monitoraggio del runtime EKS

Questa sezione si applica ai seguenti scenari:

- Non hai mai abilitato EKS Runtime Monitoring separatamente e ora hai disabilitato il Runtime Monitoring.
- Stai disabilitando sia il Runtime Monitoring che EKS Runtime Monitoring. Se non sei sicuro dello stato di configurazione di EKS Runtime Monitoring, consulta [Verifica dello stato della configurazione di EKS Runtime Monitoring](#)

 **Disabilitazione del monitoraggio del runtime senza disabilitare EKS Runtime Monitoring**
In questo scenario, a un certo punto, è stato abilitato EKS Runtime Monitoring e, successivamente, è stato abilitato anche il Runtime Monitoring senza disabilitare EKS Runtime Monitoring.
Ora, quando disabiliti il monitoraggio del runtime, dovrai disabilitare anche EKS Runtime Monitoring; in caso contrario, continuerai a sostenere costi di utilizzo per EKS Runtime Monitoring.

Se gli scenari elencati in precedenza si applicano al vostro caso, GuardDuty intraprenderemo le seguenti azioni nel vostro account:

- GuardDuty elimina l'endpoint VPC che ha GuardDutyManaged il tag: `true`. Questo è il VPC creato per gestire GuardDuty l'agente di sicurezza automatizzato.
- GuardDuty elimina il gruppo di sicurezza contrassegnato come GuardDutyManaged: `true`
- Per un VPC condiviso che è stato utilizzato da almeno un account partecipante, GuardDuty non elimina né l'endpoint VPC né il gruppo di sicurezza associato alla risorsa VPC condivisa.
- Per una risorsa Amazon EKS, GuardDuty elimina il security agent. Ciò è indipendente dal fatto che sia gestito manualmente o tramite GuardDuty.

Per una risorsa Amazon ECS, poiché un'attività ECS è immutabile, non è GuardDuty possibile disinstallare il security agent da quella risorsa. Ciò è indipendente dal modo in cui gestisci l'agente di sicurezza, manualmente o automaticamente tramite GuardDuty. Dopo aver disabilitato il monitoraggio del runtime, non GuardDuty collegherà un contenitore secondario quando inizia l'esecuzione di una nuova attività ECS. Per informazioni sull'utilizzo delle attività di Fargate-ECS, vedere [Come funziona il monitoraggio del runtime con Fargate \(solo Amazon ECS\)](#)

Per una risorsa Amazon EC2, GuardDuty disinstalla l'agente di sicurezza da tutte le istanze Amazon EC2 gestite da Systems Manager (SSM) solo quando soddisfa le seguenti condizioni:

- La tua risorsa non è etichettata con: tag di esclusione. GuardDutyManaged `false`

- GuardDuty deve disporre delle autorizzazioni per accedere ai tag nei metadati dell'istanza. Per questa risorsa EC2, l'accesso ai tag nei metadati dell'istanza è impostato su Consenti.

Quando smetti di gestire manualmente il Security Agent

Indipendentemente dall'approccio utilizzato per distribuire e gestire il GuardDuty security agent, per interrompere il monitoraggio degli eventi di runtime nella risorsa, è necessario rimuovere il GuardDuty security agent. Se desideri interrompere il monitoraggio degli eventi di runtime da un tipo di risorsa in un account, puoi anche eliminare l'endpoint Amazon VPC.

Disinstallazione manuale dell'agente di sicurezza per le risorse Amazon EC2

Questa sezione fornisce i metodi per disinstallare il GuardDuty security agent dalle risorse Amazon EC2. Quando gestisci il security agent manualmente, hai la responsabilità di rimuoverlo dalle risorse. GuardDuty non intraprenderà alcuna azione sulle risorse che gestisci.

Se hai creato un endpoint Amazon VPC manualmente, dopo aver disinstallato il security agent su tutti i tipi di risorse monitorate nel tuo account, puoi scegliere di eliminare l'endpoint VPC. Questa è una fase a parte. Per ulteriori informazioni, consulta [To delete a VPC endpoint](#).

In base a come hai installato il security agent nella tua risorsa, scegli uno dei seguenti metodi per disinstallarlo.

Argomenti

- [Metodo 1: utilizzando il comando Esegui](#)
- [Metodo 2 - Utilizzando Linux Package Managers](#)

Metodo 1: utilizzando il comando Esegui

Quando hai installato il security agent con [Metodo 1 - Utilizzo AWS Systems Manager](#), esegui le seguenti operazioni per disinstallare l'agente:

Per disinstallare il GuardDuty security agent

1. È possibile disinstallare il GuardDuty security agent seguendo i passaggi specificati in [AWS Systems Manager Esegui comando](#) nella Guida per l'AWS Systems Manager utente. Utilizzate l'azione Disinstalla nei parametri per disinstallare il GuardDuty security agent.

Nella sezione Target, assicurati che l'impatto riguardi solo le istanze Amazon EC2 da cui desideri disinstallare il security agent.

Utilizza il seguente GuardDuty documento e distributore:

- Nome del documento: AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
 - Distributore: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. Dopo aver fornito tutti i dettagli, quando scegli Run, l'agente di sicurezza che ha distribuito sulle istanze Amazon EC2 di destinazione viene rimosso.

Per rimuovere la configurazione degli endpoint Amazon VPC, devi disabilitare sia Runtime Monitoring che Amazon EKS Runtime Monitoring.

3. Se desideri eliminare anche l'endpoint VPC associato a questo security agent, consulta. [To delete a VPC endpoint](#)

Metodo 2 - Utilizzando Linux Package Managers

Quando avete installato il security agent con [Metodo 2: utilizzo dei gestori di pacchetti Linux](#), effettuate le seguenti operazioni per disinstallarlo:

Per disinstallare il GuardDuty security agent

1. Connect alla tua istanza. Per istruzioni su come eseguire questa operazione, consulta [Connect to your Linux using an SSH client](#) nella Amazon EC2 User Guide.
2. Comando di disinstallazione

Il comando seguente disinstallerà il GuardDuty security agent dall'istanza Amazon EC2 a cui ti connetti:

- Per RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Per Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Dopo aver eseguito il comando, è possibile controllare anche i log associati al comando.

3. Se desideri eliminare anche l'endpoint VPC associato a questo security agent, consulta. [To delete a VPC endpoint](#)

Pulizia delle risorse del Security Agent

Questa sezione spiega come ripulire le AWS risorse associate al Security Agent. Come elencato in [Disabilitazione, disinstallazione e pulizia delle risorse](#), non GuardDuty eliminerà o rimuoverà tutte le risorse del Security Agent. La sezione seguente fornisce istruzioni su come eliminare le risorse del Security Agent.

Per eliminare l'endpoint Amazon VPC

Quando gestisci manualmente il security agent, potresti aver creato manualmente un endpoint Amazon VPC. Dopo aver disinstallato il security agent per tutte le risorse monitorate nel tuo account, puoi scegliere di eliminare questo endpoint VPC.

L'elenco seguente fornisce scenari in cui si utilizza un VPC condiviso rispetto al non utilizzo di un VPC condiviso.

- Senza un VPC condiviso: quando non desideri più monitorare una risorsa in un account, prendi in considerazione l'eliminazione dell'endpoint Amazon VPC.
- Con un VPC condiviso: quando un account proprietario VPC condiviso elimina la risorsa VPC condivisa che era ancora in uso, lo stato di copertura del Runtime Monitoring (e, se applicabile, EKS Runtime Monitoring) per le risorse nell'account proprietario del VPC condiviso e nell'account partecipante potrebbe non funzionare correttamente. Per informazioni sullo stato della copertura, vedere. [Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi](#)

Per eliminare l'endpoint VPC, [consulta Eliminare un endpoint di interfaccia](#) nella Guida.AWS PrivateLink

Per eliminare il gruppo di sicurezza

- Senza un VPC condiviso: quando non desideri più monitorare un tipo di risorsa in un account, prendi in considerazione l'eliminazione del gruppo di sicurezza associato ad Amazon VPC.
- Con un VPC condiviso: quando l'account proprietario del VPC condiviso elimina il gruppo di sicurezza, qualsiasi account partecipante che attualmente utilizza il gruppo di sicurezza

associato al VPC condiviso, lo stato di copertura del Runtime Monitoring per le risorse nell'account proprietario del VPC condiviso e nell'account partecipante potrebbe non essere integro. Per ulteriori informazioni, consulta [Revisione delle statistiche sulla copertura del runtime e risoluzione dei problemi](#).

Per informazioni sui passaggi, consulta [Eliminare un gruppo di sicurezza Amazon EC2](#) nella Amazon EC2 User Guide.

Per rimuovere un agente GuardDuty di sicurezza da un cluster EKS

Per rimuovere l'agente di sicurezza dal cluster EKS che non desideri più monitorare, consulta [Rimuovere un componente aggiuntivo Amazon EKS da un cluster](#) nella Guida per l'utente di Amazon EKS.

La rimozione dell'agente (componente aggiuntivo EKS) non rimuove lo spazio dei nomi di amazon-guardduty dal cluster EKS. Per eliminare lo spazio dei nomi amazon-guardduty, consulta [Eliminazione di uno spazio dei nomi](#).

Per eliminare lo spazio dei **amazon-guardduty** nomi (cluster EKS)

La disabilitazione della configurazione automatizzata dell'agente non rimuove automaticamente lo spazio dei nomi amazon-guardduty dal cluster EKS. Per eliminare lo spazio dei nomi amazon-guardduty, consulta [Eliminazione di uno spazio dei nomi](#).

GuardDuty Protezione da malware per EC2

Malware Protection for EC2 ti aiuta a rilevare la potenziale presenza di malware eseguendo la scansione dei [volumi Amazon Elastic Block Store \(Amazon EBS\) collegati alle istanze Amazon Elastic Compute Cloud \(Amazon EC2\)](#) e dei carichi di lavoro dei container in esecuzione su Amazon EC2. Malware Protection for EC2 offre opzioni di scansione in cui puoi decidere se includere o escludere istanze Amazon EC2 specifiche al momento della scansione. Offre inoltre la possibilità di conservare le istantanee dei volumi Amazon EBS collegati alle istanze Amazon EC2 o ai carichi di lavoro dei container nei tuoi account. GuardDuty Le istantanee vengono conservate solo quando viene rilevato malware e vengono generati i risultati di Malware Protection for EC2.

Malware Protection for EC2 è progettato in modo da non influire sulle prestazioni delle risorse. Per informazioni su come funziona Malware Protection for EC2 all'interno GuardDuty, consulta [In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware](#) Per informazioni sulla disponibilità di Malware Protection for EC2 in diverse versioni Regioni AWS, consulta [Regioni ed endpoint](#)

Note

Malware Protection for EC2 supporta le scansioni antimalware su istanze gestite per Amazon EKS Auto Mode. Per ulteriori informazioni, consulta il supporto delle [istanze gestite](#) in Guardduty.

Malware Protection for EC2 non supporta le scansioni antimalware per i AWS Fargate carichi di lavoro in esecuzione con Amazon EKS o Amazon ECS.

Per informazioni su queste funzionalità di Amazon EKS, consulta [Cos'è Amazon EKS?](#) nella Guida per l'utente di Amazon EKS.

Argomenti

- [Confronto tra la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta](#)
- [In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware](#)
- [Volumi Amazon EBS supportati per la scansione di malware](#)
- [Configura la conservazione delle istantanee e la copertura delle scansioni EC2](#)
- [GuardDuty-scansione antimalware avviata](#)
- [Scansione antimalware su richiesta GuardDuty](#)

- [Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for EC2](#)
- [GuardDuty account di servizio di Regione AWS](#)
- [Quote nella protezione da malware per EC2](#)

Confronto tra la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta

Malware Protection for EC2 offre due tipi di scansioni per rilevare attività potenzialmente dannose nelle istanze Amazon EC2 e nei carichi di lavoro dei container GuardDuty: scansione malware avviata e scansione malware su richiesta. La tabella seguente mostra il confronto tra i due tipi di scansione.

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
Come viene richiamata la scansione	Dopo aver GuardDuty abilitato la scansione antimalware avviata, ogni volta che GuardDuty genera un risultato che indica la potenziale presenza di malware in un'istanza Amazon EC2 o in un carico di lavoro di container GuardDuty , avvia automaticamente una scansione del malware senza agenti sui volumi Amazon EBS collegati alla risorsa potenzialmente interessata. Per ulteriori informazioni, consulta GuardDuty-scansione antimalware avviata .	Puoi avviare una scansione antimalware su richiesta fornendo l'Amazon Resource Name (ARN) della tua istanza Amazon EC2. Puoi avviare una scansione antimalware su richiesta anche quando non viene generato alcun GuardDuty risultato relativo alla tua risorsa. Per ulteriori informazioni, consulta Scansione antimalware su richiesta GuardDuty .
Configurazione necessaria	Per utilizzare GuardDuty - initiated malware scan, devi abilitarla per il tuo account.	Il tuo account deve essere abilitato GuardDuty . Per utilizzare la scansione

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
	Per gestire più account utilizzando AWS Organizations un metodo basato su invito, consulta. Abilitazione della scansione GuardDuty antimalware avviata in ambienti con più account Per abilitare la scansione antimalware GuardDuty avviata dal sistema nel tuo account, consulta. Attivazione della scansione antimalware GuardDuty avviata per un account autonomo	antimalware su richiesta, non è richiesta alcuna configurazione a livello di funzionalità.
Tempo di attesa per avviare una nuova scansione	Ogni volta che ne GuardDuty genera uno Risultati che richiamano la scansione GuardDuty antimalware avviata, una scansione antimalware viene avviata automaticamente solo una volta ogni 24 ore.	È possibile avviare una scansione antimalware su richiesta sulla stessa risorsa in qualsiasi momento dopo 1 ora dall'inizio della scansione precedente.

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
Disponibilità del periodo di prova gratuito di 30 giorni ¹	Quando attivi la scansione antimalware GuardDuty avviata per la prima volta nel tuo account, puoi utilizzare un periodo di prova gratuito di 30 giorni. Per ulteriori informazioni, consulta Versione di prova gratuita di 30 giorni per la scansione antimalware avviata GuardDuty.	Non è previsto un periodo di prova gratuito con la scansione antimalware su richiesta per account nuovi o esistenti. GuardDuty
Opzioni di scansione ²	Dopo aver configurato la scansione antimalware GuardDuty avviata, Malware Protection for EC2 offre la possibilità di scansionare o ignorare risorse Amazon EC2 specifiche utilizzando i tag. Malware Protection for EC2 non avvierà una scansione automatica delle risorse che scegli di escludere dalla scansione. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente .	Poiché fornisci la risorsa ARN per avviare manualmente una scansione antimalware su richiesta, l'utilizzo Opzioni di scansione con tag definiti dall'utente non è applicabile.

¹ Dovrai sostenere i costi di utilizzo per la creazione di istantanee dei volumi EBS e la conservazione delle istantanee. Per ulteriori informazioni sulla configurazione dell'account per conservare le istantanee, consulta. [Conservazione delle istantanee](#)

² La scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta supportano l'utilizzo di un tag globale per escludere le risorse Amazon EC2 dalle scansioni antimalware. Per ulteriori informazioni, consulta [Tag GuardDutyExcluded globale](#).

In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware

Questa sezione spiega in che modo Malware Protection for EC2, inclusa la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta, analizza i volumi Amazon EBS associati alle istanze Amazon EC2 e ai carichi di lavoro dei container. Prima di procedere, considera le personalizzazioni seguenti:

- **Opzioni di scansione:** Malware Protection for EC2 offre la possibilità di specificare tag per includere o escludere le istanze Amazon EC2 e i volumi Amazon EBS dal processo di scansione. Solo la scansione antimalware GuardDuty avviata supporta opzioni di scansione con tag definiti dall'utente. Sia la scansione antimalware GuardDuty avviata che la scansione antimalware su richiesta supportano il tag globale. GuardDutyExcluded Per ulteriori informazioni, consulta [Opzioni di scansione con tag definiti dall'utente](#).
- **Conservazione delle istantanee:** Malware Protection for EC2 offre un'opzione per conservare le istantanee dei volumi Amazon EBS nel tuo account. AWS Per impostazione predefinita, questa impostazione è disattivata. È possibile attivare la conservazione delle istantanee sia per le scansioni antimalware GuardDuty avviate che per quelle su richiesta. Per ulteriori informazioni, consulta [Conservazione delle istantanee](#).

Quando ne GuardDuty genera una o più [Risultati che richiamano la scansione GuardDuty antimalware avviata](#), questa attività sarà un motivo per avviare una scansione GuardDuty antimalware. Se le opzioni di scansione non escludono questa istanza, GuardDuty avvierà la scansione.

Per avviare una scansione antimalware on demand sui volumi Amazon EBS associati a un'istanza Amazon EC2, fornisci il nome della risorsa Amazon (ARN) dell'istanza in questione.

In risposta all'avvio di una scansione antimalware su richiesta o di una scansione antimalware GuardDuty avviata automaticamente, GuardDuty crea istantanee dei volumi EBS pertinenti collegati alla risorsa potenzialmente interessata e le condivide con. [GuardDuty account di servizio](#) Quando GuardDuty crea un'istanza dei volumi EBS, aggiunge un tag predefinito chiamato. GuardDutyScanId Questo tag consente di accedere GuardDuty all'istanza. Assicurati di non

rimuovere questo tag. Da queste istantanee, GuardDuty crea una replica crittografata del volume EBS nell'account del servizio.

Al termine della scansione, GuardDuty elimina i volumi EBS di replica crittografati e le istantanee dei volumi EBS. Per impostazione predefinita, l'impostazione di conservazione delle istantanee è disattivata. Tuttavia, le istantanee vengono conservate se il [blocco degli snapshot di Amazon EBS](#) è abilitato per esse, indipendentemente dai risultati e dalle impostazioni della scansione. GuardDuty non può modificare le impostazioni del blocco degli snapshot di Amazon EBS.

L'elenco seguente descrive il comportamento di conservazione degli snapshot, indipendentemente dal blocco degli snapshot EBS:

La conservazione delle istantanee è attivata:

- Quando viene rilevato un malware, GuardDuty conserva le istantanee nel tuo Account AWS
- Quando non viene rilevato alcun malware, GuardDuty non conserva le istantanee a meno che non siano bloccate.

La conservazione delle istantanee è disattivata (impostazione predefinita):

- Indipendentemente dal fatto che venga rilevato o meno un malware, le istantanee non vengono conservate.
- GuardDuty non è possibile eliminare gli snapshot Amazon EBS bloccati.

GuardDuty conserverà ogni volume EBS di replica nell'account di servizio per un massimo di 55 ore. In caso di interruzione del servizio o di errore con un volume EBS di replica e la relativa scansione antimalware, GuardDuty conserverà tale volume EBS per non più di sette giorni. Il periodo di conservazione prolungato del volume serve a valutare e risolvere l'interruzione o l'errore. GuardDuty Malware Protection for EC2 eliminerà i volumi EBS di replica dall'account di servizio dopo aver risolto l'interruzione o l'errore o una volta scaduto il periodo di conservazione prolungato.

Per informazioni sulla metodologia di rilevamento del GuardDuty malware e sui motori di scansione utilizzati, consulta. [GuardDuty motore di scansione per il rilevamento di malware](#)

Volumi Amazon EBS supportati per la scansione di malware

Ovunque sia GuardDuty supportata la Regione AWS funzionalità Malware Protection for EC2, puoi scansionare i volumi Amazon EBS non crittografati o crittografati. Puoi avere volumi Amazon EBS crittografati con una delle due chiavi [Chiave gestita da AWS](#) o con una [chiave gestita dal cliente](#). Attualmente, alcune delle regioni in cui è disponibile Malware Protection for EC2 possono supportare

entrambi i modi di crittografare i volumi Amazon EBS, mentre altre supportano solo la chiave gestita dal cliente. Per informazioni sulle regioni supportate, consulta e. [GuardDuty account di servizio di Regione AWS](#) Per informazioni sulle regioni in cui GuardDuty è disponibile ma Malware Protection for EC2 non è disponibile, consulta [Disponibilità di funzionalità specifiche per ogni regione](#).

L'elenco seguente descrive la chiave che GuardDuty utilizza indipendentemente dal fatto che i volumi Amazon EBS siano crittografati o meno:

- Volumi Amazon EBS non crittografati o crittografati con Chiave gestita da AWS: GuardDuty utilizza la propria chiave per crittografare i volumi Amazon EBS di replica.

Se la tua regione non supporta la scansione di volumi Amazon EBS crittografati con la [crittografia Amazon EBS per impostazione predefinita](#), devi modificare la chiave predefinita in modo che diventi una chiave gestita dal cliente. Questo ti aiuterà ad GuardDuty accedere a questi volumi EBS. Modificando la chiave, anche i futuri volumi EBS verranno creati con la chiave aggiornata in modo da GuardDuty supportare le scansioni di malware. Per i passaggi per modificare la chiave predefinita, consulta [Modifica l'ID AWS KMS chiave predefinito di un volume Amazon EBS](#) la sezione successiva.

- Volumi Amazon EBS crittografati con chiave gestita dal cliente: GuardDuty utilizza la stessa chiave per crittografare il volume EBS di replica. Per informazioni su quali politiche relative alla AWS KMS crittografia sono supportate, consulta. [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#)

Modifica l'ID AWS KMS chiave predefinito di un volume Amazon EBS

Quando crei un volume Amazon EBS utilizzando la [crittografia Amazon EBS](#) e non specifichi l'ID della AWS KMS chiave, il volume Amazon EBS viene crittografato con una [chiave di crittografia predefinita](#). Quando abiliti la crittografia per impostazione predefinita, Amazon EBS crittograferà automaticamente nuovi volumi e snapshot utilizzando la tua chiave KMS predefinita per la crittografia Amazon EBS.

Puoi modificare la chiave di crittografia predefinita e utilizzare una chiave gestita dal cliente per la crittografia Amazon EBS. Ciò consentirà di GuardDuty accedere a questi volumi Amazon EBS. Per modificare l'ID predefinito della chiave EBS, aggiungi la seguente autorizzazione necessaria alla tua policy IAM: `ec2:modifyEbsDefaultKmsKeyId`. Qualsiasi volume Amazon EBS appena creato che scegli di crittografare ma che non specifica un ID chiave KMS associato, utilizzerà l'ID chiave predefinito. Utilizza uno dei seguenti metodi per aggiornare l'ID della chiave predefinita EBS:

Per modificare l'ID predefinito della chiave KMS di un volume Amazon EBS

Esegui una delle seguenti operazioni:

- Utilizzo di un'API: puoi utilizzare l'[ModifyEbsDefaultKmsKeyId](#) API. Per informazioni su come visualizzare lo stato di crittografia del volume, consulta [Create Amazon EBS volume](#).
- Utilizzo del AWS CLI comando: l'esempio seguente modifica l'ID chiave KMS predefinito che crittograferà i volumi Amazon EBS se non fornisci un ID chiave KMS. Assicurati di sostituire la regione con l'ID Regione AWS della tua chiave KM.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

Il comando precedente genererà un output simile al seguente:

```
{  
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"  
}
```

Per ulteriori informazioni, vedi [modify-ebs-default-kms-key-id](#).

Configura la conservazione delle istantanee e la copertura delle scansioni EC2

Questa sezione spiega come personalizzare le opzioni di scansione antimalware per le istanze Amazon EC2. Queste personalizzazioni si applicano sia alle scansioni antimalware su richiesta sia a quelle avviate da GuardDuty. È possibile effettuare le seguenti operazioni:

- Abilita la conservazione delle istantanee: se abilitata prima di una scansione, GuardDuty conserverà lo snapshot di Amazon EBS GuardDuty rilevato come dannoso.
- Scegli quali istanze Amazon EC2 scansionare: utilizza i tag per includere o escludere istanze Amazon EC2 specifiche dalle scansioni di malware.

Conservazione delle istantanee

GuardDuty ti offre la possibilità di conservare le istantanee dei tuoi volumi EBS nel tuo account. AWS Per impostazione predefinita, la conservazione degli snapshot è disattivata. Gli snapshot verranno conservati solo se questa impostazione viene attivata prima dell'avvio della scansione.

All'avvio della scansione, GuardDuty genera i volumi EBS di replica in base alle istantanee dei volumi EBS. Una volta completata la scansione e dopo aver già attivato l'impostazione di conservazione degli snapshot nell'account, gli snapshot dei volumi EBS verranno conservati solo in caso di rilevamento di malware e di generazione di [Protezione da malware per tipi di ricerca EC2](#). Quando non viene rilevato alcun malware, indipendentemente dalle impostazioni degli snapshot, elimina GuardDuty automaticamente gli snapshot dei volumi EBS a meno che il [blocco degli snapshot di Amazon EBS non sia stato abilitato sugli snapshot](#) creati.

Costo di utilizzo degli snapshot

Durante la scansione antimalware, durante la GuardDuty creazione delle istantanee dei volumi Amazon EBS, a questa fase è associato un costo di utilizzo. Se attivi l'impostazione di conservazione degli snapshot per il tuo account, quando viene rilevato un malware dovrai sostenere i costi di utilizzo per conservare gli snapshot. Per informazioni sul costo degli snapshot e sulla loro conservazione, consulta i prezzi di [Amazon EBS](#).

In qualità di account GuardDuty amministratore delegato, solo tu puoi effettuare questo aggiornamento per conto degli account dei membri dell'organizzazione. Tuttavia, se un account membro è [gestito tramite il metodo di invito](#), può apportare questa modifica autonomamente. Per ulteriori informazioni, consulta [Relazioni tra account amministratore e account membro](#).

Scegli il metodo di accesso che preferisci per attivare l'impostazione di conservazione degli snapshot.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione, sotto Piani di protezione, scegli Malware Protection for EC2.
3. Scegli Impostazioni generali nella sezione inferiore della console. Per conservare gli snapshot, attiva la Conservazione degli snapshot.

API/CLI

Esegui [UpdateMalwareScanSettings](#) per aggiornare la configurazione corrente per l'impostazione di conservazione delle istantanee.

In alternativa, puoi eseguire il seguente AWS CLI comando per conservare automaticamente le istantanee quando GuardDuty Malware Protection for EC2 genera dei risultati.

Assicurati di sostituirla *detector-id* con una tua valida. detectorId

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Se desideri disattivare la conservazione degli snapshot, sostituisci RETENTION_WITH_FINDING con NO_RETENTION.

Opzioni di scansione con tag definiti dall'utente

Utilizzando GuardDuty -initiated malware scan, puoi anche specificare tag per includere o escludere le istanze Amazon EC2 e i volumi Amazon EBS dal processo di scansione e rilevamento delle minacce. Puoi personalizzare ogni scansione antimalware GuardDuty avviata modificando i tag nell'elenco dei tag di inclusione o di esclusione. Ogni elenco può includere fino a 50 tag.

Se non disponi già di tag definiti dall'utente associati alle tue risorse EC2, consulta [Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide](#).

Note

La scansione antimalware on demand non supporta le opzioni di scansione con tag definiti dall'utente. Supporta [Tag GuardDutyExcluded globale](#).

Per escludere istanze EC2 dalla scansione malware

Se desideri escludere un'istanza Amazon EC2 o un volume Amazon EBS durante il processo di scansione, puoi impostare il `GuardDutyExcluded` tag su qualsiasi istanza Amazon EC2 o volume Amazon EBS e non eseguirai la scansione. `true` GuardDuty Per ulteriori informazioni sul tag `GuardDutyExcluded`, consulta [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#). Puoi anche aggiungere un tag di istanza Amazon EC2 a un elenco di esclusione. Se aggiungi più tag all'elenco dei tag di esclusione, qualsiasi istanza Amazon EC2 che contiene almeno uno di questi tag verrà esclusa dal processo di scansione del malware.

In qualità di account GuardDuty amministratore delegato, solo tu puoi effettuare questo aggiornamento per conto degli account dei membri dell'organizzazione. Tuttavia, se un account membro è [gestito tramite il metodo di invito](#), può apportare questa modifica autonomamente. Per ulteriori informazioni, consulta [Relazioni tra account amministratore e account membro](#).

Scegli il metodo di accesso che preferisci per aggiungere un tag associato a un'istanza Amazon EC2 a un elenco di esclusione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione, sotto Piani di protezione, scegli Malware Protection for EC2.
3. Espandi la sezione Tag di inclusione/esclusione. Scegli Aggiungi tag.
4. Scegli Tag di esclusione, quindi Conferma.
5. Specifica la coppia di **Key** e **Value** del tag che desideri escludere. Fornire il **Value** è facoltativo. Dopo aver aggiunto tutti i tag, scegli Salva.



Important

Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta [Restrizioni relative ai tag](#) nella Guida per l'utente di Amazon EC2.

Se non viene fornito un valore per una chiave e l'istanza EC2 è etichettata con la chiave specificata, questa istanza EC2 verrà esclusa dal processo di scansione antimalware GuardDuty avviato, indipendentemente dal valore assegnato al tag.

API/CLI

Eseguita [UpdateMalwareScanSettings](#) escludendo un'istanza EC2 o un carico di lavoro del contenitore dal processo di scansione.

Il seguente comando di AWS CLI esempio aggiunge un nuovo tag all'elenco dei tag di esclusione. Sostituisci il *detector-id* di esempio con il tuo detectorId valido.

MapEquals è un elenco di coppie Key/Value.

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
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

Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta [Restrizioni relative ai tag](#) nella Guida per l'utente di Amazon EC2.

Per includere istanze EC2 nella scansione malware

Se desideri scansionare un'istanza EC2, aggiungi il relativo tag all'elenco di inclusione. Quando aggiungi un tag a un elenco di tag di inclusione, un'istanza EC2 che non contiene nessuno dei tag aggiunti viene ignorata durante la scansione malware. Se aggiungi più tag all'elenco dei tag di inclusione, un'istanza EC2 che contiene almeno uno di questi tag viene inclusa nella scansione malware. A volte, un'istanza EC2 può essere ignorata durante il processo di scansione per altri motivi. Per ulteriori informazioni, consulta [Motivi per cui una risorsa viene ignorata durante la scansione malware](#).

In qualità di account GuardDuty amministratore delegato, solo tu puoi effettuare questo aggiornamento per conto degli account dei membri dell'organizzazione. Tuttavia, se un account

membro è [gestito tramite il metodo di invito](#), può apportare questa modifica autonomamente. Per ulteriori informazioni, consulta [Relazioni tra account amministratore e account membro](#).

Scegli il metodo di accesso che preferisci per aggiungere un tag associato a un'istanza EC2 a un elenco di inclusione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione, sotto Piani di protezione, scegli Malware Protection for EC2.
3. Espandi la sezione Tag di inclusione/esclusione. Scegli Aggiungi tag.
4. Scegli Tag di inclusione, quindi Conferma.
5. Scegli Aggiungi nuovo tag di inclusione e specifica la coppia di **Key** e **Value** del tag che desideri includere. Fornire il **Value** è facoltativo.

Dopo aver aggiunto tutti i tag di inclusione, scegli Salva.

Se non viene fornito un valore per una chiave, un'istanza EC2 viene etichettata con la chiave specificata, l'istanza EC2 verrà inclusa nel processo di scansione di Malware Protection for EC2, indipendentemente dal valore assegnato al tag.

API/CLI

- Esegui [UpdateMalwareScanSettings](#) per includere un'istanza EC2 o un carico di lavoro del contenitore nel processo di scansione.

Il seguente comando di AWS CLI esempio aggiunge un nuovo tag all'elenco dei tag di inclusione. Assicurati di sostituire l'esempio *detector-id* con il tuo validodetectorId. Sostituisci l'esempio *TestKey* e *TestValue* con la Value coppia Key e del tag associata alla tua risorsa EC2.

MapEquals è un elenco di coppie Key/Value.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui l'[ListDetectorsAPI](#).

```
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

Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta [Restrizioni relative ai tag](#) nella Guida per l'utente di Amazon EC2.

Note

Potrebbero essere necessari fino a 5 minuti per GuardDuty rilevare un nuovo tag.

In qualsiasi momento, puoi scegliere tra i Tag di inclusione o i Tag di esclusione, ma non entrambi. Se desideri passare da un tag all'altro, scegilo dal menu a discesa quando aggiungi nuovi tag e Conferma la selezione. Questa operazione cancella tutti i tag correnti.

Tag **GuardDutyExcluded** globale

GuardDuty utilizza una chiave di tag globale `GuardDutyExcluded`, che puoi aggiungere alle tue risorse Amazon EC2 e su cui impostare il valore del tag. `true` Questa risorsa Amazon EC2 con questa coppia di tag, chiave e valore verrà esclusa dalla scansione del malware. Entrambi i tipi di scansione (scansione antimalware GuardDuty avviata e scansione antimalware su richiesta) supportano il tag globale. Se avvii una scansione antimalware su richiesta su Amazon EC2, verrà generato un ID di scansione. Tuttavia, la scansione verrà ignorata con un motivo. `EXCLUDED_BY_SCAN_SETTINGS` Per ulteriori informazioni, consulta [Motivi per cui una risorsa viene ignorata durante la scansione malware](#).

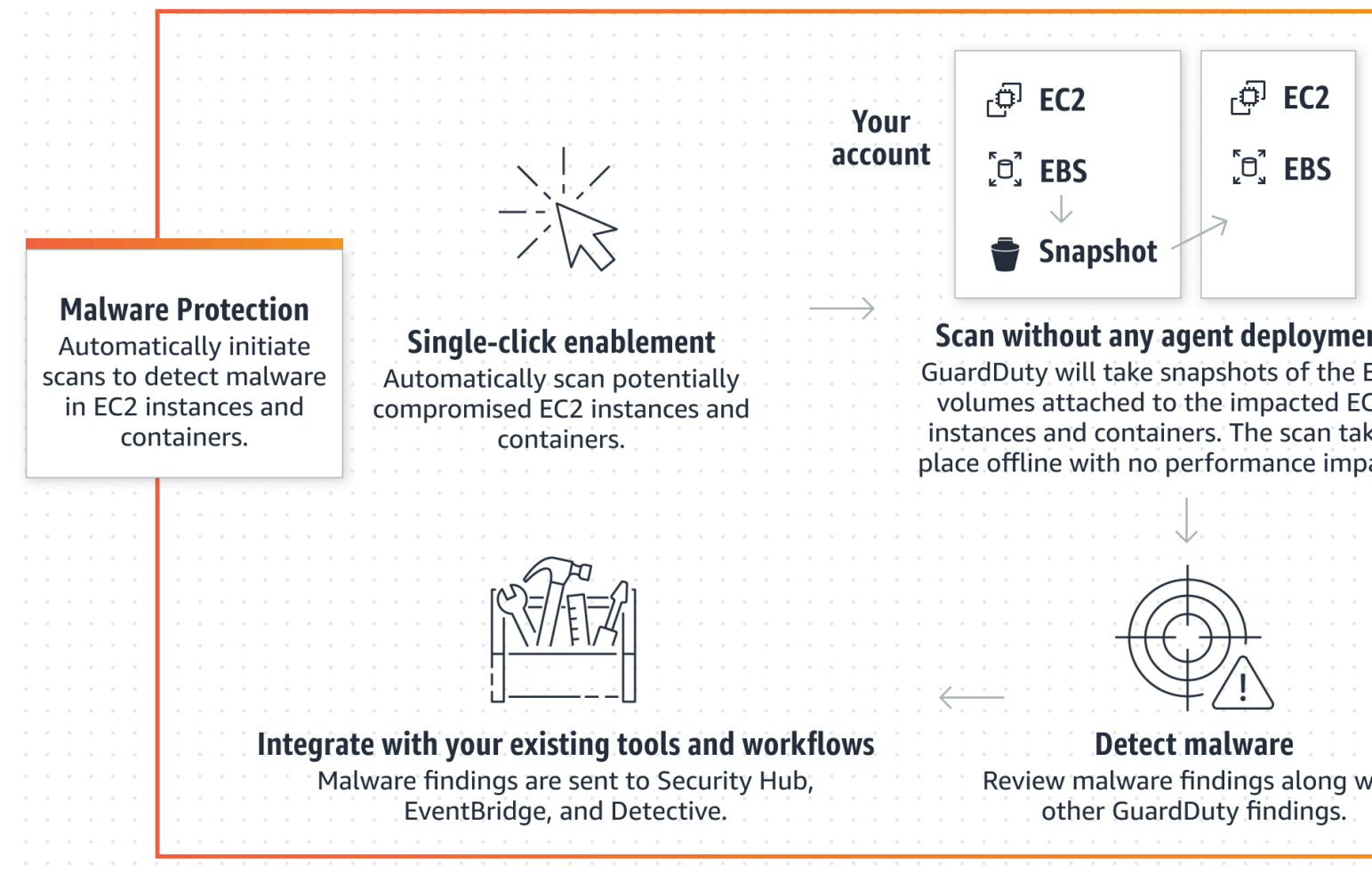
GuardDuty-scansione antimalware avviata

Con la scansione antimalware GuardDuty avviata abilitata, ogni volta che GuardDuty viene generata [Risultati che richiamano la scansione GuardDuty antimalware avviata](#), verrà avviata una scansione antimalware senza agente sui volumi Amazon Elastic Block Store (Amazon EBS) collegati alla risorsa Amazon EC2 potenzialmente interessata. Prima di iniziare una scansione, devi preparare

il tuo account per eventuali personalizzazioni. Con le opzioni di scansione, puoi aggiungere tag di inclusione associati alle risorse che desideri scansionare o aggiungere tag di esclusione associati alle risorse che desideri saltare dal processo di scansione. L'avvio automatico della scansione prenderà sempre in considerazione le opzioni di scansione disponibili. GuardDuty supporta anche una coppia globale `GuardDutyExcluded: true` tag key:value. Quando aggiungi questo tag globale a una risorsa Amazon EC2, avvia GuardDuty la scansione e poi la salta. Puoi anche scegliere di attivare l'impostazione di conservazione delle istantanee per conservare le istantanee dei tuoi volumi EBS in cui è stato potenzialmente rilevato malware. Per ulteriori informazioni sulle opzioni di scansione, sul tag di esclusione globale e sulle impostazioni delle istantanee, consulta [Configura la conservazione delle istantanee e la copertura delle scansioni EC2](#)

Quando GuardDuty genera più risultati per la stessa risorsa Amazon EC2, GuardDuty sarà in grado di avviare una scansione solo dopo che sono trascorse 24 ore dall'ultima scansione GuardDuty antimalware avviata. Per informazioni su come vengono scansionati i volumi Amazon EBS collegati all'istanza Amazon EC2 o al carico di lavoro di un container, consulta [In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware](#).

L'immagine seguente descrive come funziona la scansione antimalware GuardDuty avviata.



Per informazioni sulla metodologia di rilevamento del GuardDuty malware e sui motori di scansione utilizzati, consulta [GuardDuty motore di scansione per il rilevamento di malware](#)

Quando viene rilevato un malware, GuardDuty genera [Protezione da malware per tipi di ricerca EC2](#). Se GuardDuty non genera un risultato indicativo della presenza di malware sulla stessa risorsa, non verrà richiamata alcuna scansione antimalware GuardDuty avviata. Puoi anche avviare una scansione antimalware on demand sulla stessa risorsa. Per ulteriori informazioni, consulta [Scansione antimalware su richiesta GuardDuty](#).

Versione di prova gratuita di 30 giorni per la scansione antimalware avviata GuardDuty

Puoi scegliere di abilitare o disabilitare la scansione antimalware GuardDuty avviata per un accesso supportato Account AWS in qualsiasi Regione AWS momento. Se hai un'organizzazione, ogni account membro ha la propria prova gratuita di 30 giorni.

Per capire come funziona la prova gratuita di 30 giorni, considera i seguenti scenari:

- Quando si abilita GuardDuty per la prima volta (nuovo GuardDuty account), viene abilitata anche la scansione antimalware GuardDuty avviata, inclusa nella versione di prova gratuita di 30 giorni associata al servizio. GuardDuty
- Un GuardDuty account esistente può abilitare la scansione antimalware GuardDuty avviata per la prima volta con una prova gratuita di 30 giorni. Quando attivi questa funzionalità in un'altra regione per la prima volta, riceverai una prova gratuita di 30 giorni in quella regione.
- Se utilizzi Malware Protection for EC2 da Regione AWS prima che questo piano di protezione fosse diviso in due tipi di scansione, la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta, puoi continuare a utilizzare la scansione antimalware GuardDuty avviata con lo stesso modello di prezzo e nello stesso momento. Regione AWS Se abiliti la scansione antimalware GuardDuty avviata per la prima volta in una nuova regione, il tuo account riceverà una prova gratuita di 30 giorni.

Note

Anche se è in corso un periodo di prova gratuito di 30 giorni, si applicano i costi di utilizzo standard per la creazione degli snapshot dei volumi Amazon EBS e la loro conservazione. Per ulteriori informazioni, consulta [Prezzi di Amazon EBS](#).

Abilitazione della scansione GuardDuty antimalware avviata in ambienti con più account

In un ambiente con più account, solo gli account GuardDuty amministratore possono abilitare la scansione antimalware GuardDuty avviata per conto dei propri account membri. Inoltre, un account amministratore che gestisce gli account dei membri con AWS Organizations supporto può scegliere di abilitare automaticamente la scansione antimalware GuardDuty avviata su tutti gli account esistenti e nuovi dell'organizzazione. Per ulteriori informazioni, consulta [Gestione GuardDuty degli account con AWS Organizations](#).

Stabilire un accesso affidabile per abilitare la scansione GuardDuty antimalware avviata

Se l'account di amministratore GuardDuty delegato non è lo stesso dell'account di gestione dell'organizzazione, l'account di gestione deve abilitare la scansione antimalware GuardDuty avviata

dall'organizzazione. In questo modo, l'account amministratore delegato può creare gli account dei membri [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#) interni gestiti tramite AWS Organizations

 Note

Prima di designare un account GuardDuty amministratore delegato, consulta [Considerazioni e raccomandazioni](#)

Scegliete il metodo di accesso preferito per consentire all'account GuardDuty amministratore delegato di abilitare la scansione antimalware GuardDuty avviata dagli account dei membri dell'organizzazione.

Console

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>

Per accedere, utilizza l'account di gestione della tua AWS Organizations organizzazione.

2. a. Se non hai designato un account GuardDuty amministratore delegato, allora:

Nella pagina Impostazioni, in Account GuardDuty amministratore delegato, inserisci le 12 cifre **account ID** che desideri designare per amministrare la politica nella tua organizzazione. GuardDuty Scegli Delega.

- b. i. Se hai già designato un account GuardDuty amministratore delegato diverso dall'account di gestione, allora:

Nella pagina Impostazioni, in Amministratore delegato, attiva l'impostazione Autorizzazioni. Questa azione consentirà all'account GuardDuty amministratore delegato di allegare le autorizzazioni pertinenti agli account dei membri e di abilitare la scansione antimalware GuardDuty avviata in tali account membro.

- ii. Se hai già designato un account GuardDuty amministratore delegato uguale all'account di gestione, puoi abilitare direttamente la scansione GuardDuty antimalware avviata per gli account dei membri. Per ulteriori informazioni, consulta [Attiva automaticamente la scansione antimalware GuardDuty avviata per tutti gli account dei membri](#).

 Tip

Se l'account GuardDuty amministratore delegato è diverso dal tuo account di gestione, devi fornire le autorizzazioni all'account GuardDuty amministratore delegato per consentire l'attivazione della scansione GuardDuty antimalware avviata per gli account dei membri.

3. Se desideri consentire all'account GuardDuty amministratore delegato di abilitare la scansione antimalware GuardDuty avviata per gli account dei membri in altre regioni, modifica la tua e ripeti i passaggi precedenti. Regione AWS

API/CLI

1. Esegui il comando seguente tramite le credenziali dell'account di gestione:

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (Facoltativo) per abilitare la scansione antimalware GuardDuty avviata dall'account di gestione che non è un account amministratore delegato, l'account di gestione la creerà prima [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#) esplicitamente nel proprio account, quindi abiliterà la scansione antimalware GuardDuty avviata dall'account amministratore delegato, in modo analogo a qualsiasi altro account membro.

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. L'account amministratore delegato è stato designato nell'account attualmente selezionato GuardDuty . Regione AWS Se hai designato un account come account GuardDuty amministratore delegato in una regione, quell'account deve essere il tuo account GuardDuty amministratore delegato in tutte le altre regioni. Ripeti la fase precedente per tutte le altre regioni.

Configurazione della scansione GuardDuty antimalware avviata per l'account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per abilitare o disabilitare la scansione antimalware GuardDuty avviata per un account amministratore delegato. GuardDuty

Console

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel riquadro di navigazione, scegli Malware Protection for EC2.
3. Nella pagina Malware Protection for EC2, scegli Modifica accanto a GuardDuty-initiated malware scan.
4. Esegui una delle seguenti operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Scegli Save (Salva).

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Scegli Save (Salva).

API/CLI

Esegui l'operazione [updateDetector](#)API utilizzando il tuo ID di rilevamento regionale e passando l'featuresoggetto di tanto in name tantoEBS_MALWARE_PROTECTION. status ENABLED

È possibile abilitare GuardDuty -initiated malware scan eseguendo il comando seguente. AWS CLI Assicurati di utilizzare un account GuardDuty amministratore delegato valido. *detector ID*

Per trovare l'detectorIdaccount e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#)API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /  
    --account-ids 555555555555 /  
    --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Attiva automaticamente la scansione antimalware GuardDuty avviata per tutti gli account dei membri

Scegli il metodo di accesso preferito per abilitare la funzionalità di scansione antimalware GuardDuty avviata per tutti gli account membri. inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

Utilizzo della pagina Malware Protection for EC2

1. Nel riquadro di navigazione, scegli Malware Protection for EC2.
2. Nella pagina Malware Protection for EC2, scegli Modifica nella sezione relativa alla scansione GuardDutyantimalware avviata.
3. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente la scansione antimalware GuardDuty avviata sia per gli account esistenti che per quelli nuovi dell'organizzazione.
4. Scegli Save (Salva).

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).

2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account sottoposti alla scansione GuardDutyantimalware avviata.
4. Nella pagina Malware Protection for EC2, scegli Modifica nella sezione GuardDuty - initiated malware scan.
5. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente la scansione antimalware GuardDuty avviata sia per gli account esistenti che per quelli nuovi dell'organizzazione.
6. Scegli Save (Salva).

 Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account sottoposti alla scansione GuardDutyantimalware avviata.
4. Scegli Save (Salva).

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta [Abilita selettivamente la scansione antimalware GuardDuty avviata dagli account dei membri](#).

API/CLI

- Per abilitare selettivamente la scansione antimalware GuardDuty avviata dall'utente per i tuoi account membri, richiama l'operazione API utilizzando la tua [updateMemberDetectors](#)*detector ID*

- L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un solo utente. Per disabilitare un account membro, sostituisci ENABLED con DISABLED.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti

Scegliete il metodo di accesso preferito per abilitare la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti nell'organizzazione.

Per configurare la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, scegli Malware Protection for EC2.
3. In Malware Protection for EC2, puoi visualizzare lo stato corrente della configurazione di scansione GuardDuty antimalware avviata. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Save (Salva).

Attiva automaticamente la scansione GuardDuty antimalware avviata per gli account dei nuovi membri

Gli account membri appena aggiunti devono essere abilitati GuardDuty prima di selezionare la configurazione GuardDuty della scansione antimalware avviata. Gli account membri gestiti su invito possono configurare manualmente la scansione antimalware GuardDuty avviata per i propri account. Per ulteriori informazioni, consulta [Step 3 - Accept an invitation](#).

Scegliete il metodo di accesso preferito per abilitare la scansione antimalware GuardDuty avviata dai nuovi account che entrano a far parte della vostra organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare la scansione antimalware GuardDuty avviata per gli account dei nuovi membri di un'organizzazione, utilizzando la pagina Malware Protection for EC2 o Accounts.

Per abilitare automaticamente la scansione antimalware GuardDuty avviata per i nuovi account dei membri

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

- Utilizzo della pagina Malware Protection for EC2:

1. Nel pannello di navigazione, scegli Malware Protection for EC2.
2. Nella pagina Malware Protection for EC2, scegli Modifica nella scansione GuardDuty antimalware avviata.
3. Scegli Configura gli account manualmente.
4. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, la scansione antimalware GuardDuty avviata venga automaticamente abilitata per tale account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
5. Scegli Save (Salva).

- Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
3. Nella finestra Gestisci le preferenze di attivazione automatica, seleziona Abilita per nuovi account nella sezione GuardDuty-initiated malware scan.
4. Scegli Save (Salva).

API/CLI

- Per abilitare o disabilitare la scansione antimalware GuardDuty avviata per i nuovi account membri, richiama l'operazione API utilizzando la [UpdateOrganizationConfiguration](#) tua *detector ID*.
- L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata per un singolo account membro. Per disabilitarlo, consulta [Abilita selettivamente la scansione antimalware GuardDuty avviata dagli account dei membri](#). Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta AutoEnable su NONE.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name": "EBS_MALWARE_PROTECTION", "AutoEnable": NEW
```

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita selettivamente la scansione antimalware GuardDuty avviata dagli account dei membri

Scegli il tuo metodo di accesso preferito per configurare selettivamente la scansione antimalware GuardDuty avviata per gli account dei membri.

Console

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, controlla lo stato del tuo account membro nella colonna «GuardDutyInitiated Malware Scan».
4. Seleziona l'account per il quale desideri configurare GuardDuty -initiated malware scan. Puoi selezionare più account alla volta.
5. Dal menu Modifica piani di protezione, scegli l'opzione appropriata per GuardDuty-initiated malware scan.

API/CLI

Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata per i tuoi account membri, richiama l'operazione API utilizzando la [updateMemberDetectors](#) tua. *detector ID*

L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un singolo account membro.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Per abilitare selettivamente la scansione antimalware GuardDuty avviata dagli account dei tuoi membri, esegui l'operazione [updateMemberDetectors](#) API utilizzando la tua. *detector ID*
L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata per un singolo account membro.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita la scansione antimalware GuardDuty avviata per gli account esistenti nell'organizzazione gestiti tramite invito

Il ruolo SLR (GuardDuty Malware Protection for EC2 service-linked role) deve essere creato negli account dei membri. L'account amministratore non può abilitare la funzionalità di scansione antimalware GuardDuty avviata dagli account dei membri che non sono gestiti da. AWS Organizations

Attualmente, è possibile eseguire i seguenti passaggi tramite la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/> per abilitare la scansione antimalware GuardDuty avviata dagli account membri esistenti.

Console

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>

Accedi utilizzando le credenziali del tuo account amministratore.

2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona l'account membro per il quale desideri abilitare la scansione GuardDuty antimalware avviata. Puoi selezionare più account alla volta.
4. Scegli Azioni.
5. Scegli Disassocia membro.
6. Nel tuo account membro, nel riquadro di navigazione, scegli Protezione da malware in Piani di protezione.

7. Scegli Abilita la scansione GuardDuty antimalware avviata. GuardDuty creerà una reflex per l'account del membro. Per ulteriori informazioni sul ruolo collegato ai servizi, consulta [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#).
8. Nel tuo account amministratore, scegli Account nel pannello di navigazione.
9. Scegli l'account membro da aggiungere nuovamente all'organizzazione.
10. Scegli Operazioni, quindi Aggiungi membro.

API/CLI

1. Utilizza l'account amministratore per eseguire l'[DisassociateMembers](#) API sugli account dei membri che desiderano abilitare la scansione GuardDuty antimalware avviata.
2. Usa il tuo account membro per invocare e [UpdateDetector](#) abilitare la scansione GuardDuty antimalware avviata.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'API. [ListDetectors](#)

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Utilizza l'account amministratore per eseguire l'[CreateMembers](#) API e aggiungere nuovamente il membro all'organizzazione.

Attivazione della scansione antimalware GuardDuty avviata per un account autonomo

Un account indipendente ha la facoltà di decidere se attivare o disattivare un piano di protezione all'interno del proprio Account AWS account specifico. Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione della scansione GuardDuty antimalware avviata in ambienti con più account](#).

Dopo aver GuardDuty abilitato la scansione antimalware avviata, GuardDuty avvierà una scansione antimalware del volume Amazon EBS collegato all'istanza Amazon EC2 coinvolta in un. GuardDuty

Per un elenco dei risultati che avviano la scansione del malware, consulta. [Risultati che richiamano la scansione GuardDuty antimalware avviata](#)

Scegliete il metodo di accesso preferito per configurare la scansione antimalware GuardDuty avviata per un account indipendente.

Console

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel pannello di navigazione, sotto Piani di protezione, scegli Malware Protection for EC2.
3. Il riquadro Malware Protection for EC2 elenca lo stato attuale della scansione antimalware GuardDuty avviata per il tuo account. Scegli Abilita per abilitare la scansione antimalware GuardDuty avviata in questo account.
4. Scegli Salva per confermare la selezione.

API/CLI

Esegui l'operazione [updateDetector](#)API utilizzando il tuo ID di rilevamento regionale e passando l'dataSourceoggetto con EbsVolumes set to true.

Puoi anche abilitare GuardDuty -initiated malware scan AWS CLI utilizzando il seguente comando. AWS CLI Assicurati di usare il tuo codice valido. *detector ID*

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/>console o esegui l'[ListDetectors](#)API.

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

Risultati che richiamano la scansione GuardDuty antimalware avviata

Quando GuardDuty rileva un comportamento sospetto indicativo di malware su un'istanza Amazon EC2 o un carico di lavoro di container in esecuzione su un'istanza Amazon EC2, genererà un risultato. GuardDuty Se il risultato generato appartiene al seguente elenco di GuardDuty risultati, GuardDuty avvierà automaticamente la scansione del malware sui volumi Amazon EBS collegati all'istanza Amazon EC2 coinvolta nel rilevamento. Dopo la scansione, se GuardDuty rileva un malware, ne genererà anche uno o più. [Protezione da malware per tipi di ricerca EC2](#)

Se nel tuo account viene generato uno dei seguenti GuardDuty risultati, GuardDuty avvierà automaticamente la scansione del malware nel volume Amazon EBS dell'istanza Amazon EC2 potenzialmente compromessa.

- [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/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](#) (solo in uscita)
- [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](#) (solo in uscita)
- [UnauthorizedAccess:EC2/SSHBruteForce](#) (solo in uscita)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CAActivity.B](#)
- [Backdoor:Runtime/C&CAActivity.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](#)

Scansione antimalware su richiesta GuardDuty

La scansione antimalware on demand è utile per rilevare la presenza di malware sui volumi Amazon Elastic Block Store (Amazon EBS) collegati alle istanze Amazon EC2. Senza necessità di configurazione, puoi avviare una scansione antimalware su richiesta fornendo l'Amazon Resource Name (ARN) dell'istanza Amazon EC2 che desideri scansionare. Puoi avviare una scansione antimalware su richiesta tramite la console o l' GuardDuty API. Prima di avviare una scansione antimalware on demand, puoi impostare l'impostazione di [Conservazione delle istantanee](#) che preferisci. I seguenti scenari possono aiutarti a identificare quando utilizzare il tipo di scansione antimalware On-demand con: GuardDuty

- Vuoi rilevare la presenza di malware nelle tue istanze Amazon EC2 senza abilitare la scansione GuardDuty antimalware avviata.
- Hai abilitato la scansione antimalware GuardDuty avviata e una scansione è stata richiamata automaticamente. Dopo aver seguito la correzione consigliata per il tipo di risultato generato da Malware Protection for EC2, se desideri avviare una scansione sulla stessa risorsa, puoi avviare una scansione antimalware su richiesta dopo che è trascorsa 1 ora dall'ora di inizio della scansione precedente.

La scansione antimalware su richiesta non richiede che siano trascorse 24 ore dal momento in cui è stata avviata la scansione antimalware precedente. Deve trascorrere 1 ora prima di avviare una scansione antimalware on demand sulla stessa risorsa. Per evitare di duplicare una scansione malware sulla stessa istanza EC2, consulta [Nuova scansione dell'istanza Amazon EC2 precedentemente scansionata](#).

Note

La scansione antimalware su richiesta non è inclusa nel periodo di prova gratuito di 30 giorni con GuardDuty. Il costo di utilizzo si applica al volume totale di Amazon EBS scansionato per

ogni scansione malware. Per ulteriori informazioni, consulta i [GuardDuty prezzi di Amazon](#). Per informazioni sui costi relativi alla creazione e alla conservazione degli snapshot dei volumi Amazon EBS, consulta [Prezzi di Amazon EBS](#).

Come funziona la scansione antimalware on demand

Con On-demand Malware Scan, puoi avviare una richiesta di scansione malware per la tua istanza Amazon EC2 anche quando è attualmente in uso. Dopo aver avviato una scansione antimalware su richiesta, GuardDuty crea istantanee dei volumi Amazon EBS collegati all'istanza Amazon EC2 il cui Amazon Resource Name (ARN) è stato fornito per la scansione. Successivamente, GuardDuty condivide queste istantanee con. [GuardDuty account di servizio](#) GuardDuty crea volumi EBS di replica crittografati da tali istantanee nell'account del servizio. GuardDuty Per ulteriori informazioni su come vengono scansionati i volumi Amazon EBS, consulta [In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware](#).

Note

GuardDuty crea le istantanee dei dati che sono già stati scritti nei volumi Amazon EBS al momento dell'avvio di una scansione antimalware su richiesta.

Se viene rilevato un malware e hai abilitato l'impostazione di conservazione degli snapshot, gli snapshot del volume EBS vengono automaticamente conservati nel tuo Account AWS. La scansione antimalware on demand genera [Protezione da malware per tipi di ricerca EC2](#). Se non viene rilevato alcun malware, indipendentemente dall'impostazione di conservazione, gli snapshot dei volumi EBS vengono eliminati.

GuardDuty utilizza una chiave di tag globale `GuardDutyExcluded`, che puoi aggiungere alle tue risorse Amazon EC2 e su cui impostare il valore del tag. `true` Questa risorsa Amazon EC2 con questa coppia di tag, chiave e valore verrà esclusa dalla scansione del malware. Entrambi i tipi di scansione (scansione antimalware GuardDuty avviata e scansione antimalware su richiesta) supportano il tag globale. Se avvii una scansione antimalware su richiesta su Amazon EC2, verrà generato un ID di scansione. Tuttavia, la scansione verrà ignorata con un motivo. `EXCLUDED_BY_SCAN_SETTINGS` Per ulteriori informazioni, consulta [Motivi per cui una risorsa viene ignorata durante la scansione malware](#).

Avvio della scansione antimalware su richiesta in GuardDuty

Questa sezione fornisce un elenco di prerequisiti prima di avviare una scansione antimalware su richiesta e i passaggi per avviare la scansione su una risorsa per la prima volta.

In qualità di account GuardDuty amministratore, puoi avviare una scansione antimalware su richiesta per conto degli account dei membri attivi che hanno i seguenti prerequisiti impostati nei rispettivi account. Gli account autonomi e gli account membro attivi GuardDuty possono anche avviare una scansione antimalware su richiesta per le proprie istanze Amazon EC2.

Prerequisiti

Prima di avviare una scansione antimalware su richiesta, il tuo account deve soddisfare i seguenti prerequisiti:

- GuardDuty deve essere abilitato nel Regione AWS punto in cui desideri avviare la scansione antimalware su richiesta.
- Assicurati che sia presente il collegamento tra [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#) e l'utente IAM o il ruolo IAM. Avrai bisogno della chiave di accesso e della chiave segreta associate all'utente IAM o al ruolo IAM.
- In qualità di account GuardDuty amministratore delegato, hai la possibilità di avviare una scansione antimalware su richiesta per conto di un account membro attivo.
- Prima di avviare una scansione antimalware su richiesta, assicurati che non sia stata avviata alcuna scansione sulla stessa risorsa nell'ultima ora; in caso contrario, verrà deduplicata. Per ulteriori informazioni, consulta [Nuova scansione dell'istanza Amazon EC2 precedentemente scansionata](#).
- Se sei un account membro che non dispone di [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#), l'avvio di una scansione antimalware su richiesta per un'istanza Amazon EC2 che appartiene al tuo account creerà automaticamente la SLR for Malware Protection for EC2.

Important

Assicurati che nessuno elimini le [autorizzazioni SLR per Malware Protection for EC2 quando la scansione antimalware](#) è ancora in corso. Questa scansione antimalware può

essere avviata da GuardDuty o avviata su richiesta. L'eliminazione della reflex impedirà il completamento corretto della scansione e fornirà un risultato di scansione definitivo.

Avvia la scansione antimalware su richiesta

Puoi avviare una scansione antimalware su richiesta nel tuo account tramite GuardDuty console o utilizzando AWS CLI. Dovrai fornire l'Amazon Resource Name (ARN) di Amazon EC2 per cui desideri avviare la scansione. I passaggi dettagliati sono forniti sia nella console che nelle AWS CLI istruzioni API/ nella sezione seguente.

Scegliete il metodo di accesso preferito per avviare una scansione antimalware su richiesta.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Avvia la scansione utilizzando una delle seguenti opzioni:
 - a. Utilizzo della pagina Malware Protection for EC2:
 - i. Nel pannello di navigazione, sotto Piani di protezione, scegli Malware Protection for EC2.
 - ii. Nella pagina Malware Protection for EC2, fornisci l'ARN 1 dell'istanza Amazon EC2 per cui desideri avviare la scansione.
 - b. Utilizzando la pagina Scansioni malware:
 - i. Nel riquadro di navigazione, scegli Scansioni malware.
 - ii. Scegli Avvia scansione su richiesta e fornisci l'ARN 1 dell'istanza Amazon EC2 per cui desideri avviare la scansione.
 - iii. Se si tratta di una nuova scansione, seleziona un ID istanza Amazon EC2 nella pagina Scansioni malware.

Espandi il menu a discesa Avvia scansione on demand e scegli Esegui nuovamente la scansione dell'istanza selezionata.
3. Dopo aver avviato correttamente una scansione utilizzando uno dei due metodi, viene generato un ID di scansione che può essere utilizzato per tenere traccia dello stato di avanzamento della scansione. Per ulteriori informazioni, consulta [Monitoraggio dello stato e del risultato delle scansioni malware](#).

API/CLI

Invoke [StartMalwareScan](#) that accetta l'^{istanza} 1 resourceArn di Amazon EC2 per la quale desideri avviare una scansione antimalware su richiesta.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

Dopo aver avviato correttamente una scansione, StartMalwareScan restituisce un. scanId
Invoke [DescribeMalwareScans](#) monitora lo stato di avanzamento della scansione avviata.

¹Per informazioni sul formato dell'ARN dell'istanza Amazon EC2, consulta [Nome della risorsa Amazon \(ARN\)](#). Per le istanze Amazon EC2, puoi utilizzare il seguente formato ARN di esempio sostituendo i valori per la partizione, la regione, l'ID Account AWS e l'ID dell'istanza Amazon EC2. Per informazioni sulla lunghezza dell'ID dell'istanza, consulta [Resource IDs](#).

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

AWS Organizations politica di controllo del servizio: accesso negato

Utilizzando le [policy di controllo del servizio \(SCPs\)](#) in AWS Organizations, l'account GuardDuty amministratore delegato può limitare le autorizzazioni e negare azioni come l'avvio di una scansione antimalware su richiesta per l'istanza Amazon EC2 di proprietà dei tuoi account.

Come account GuardDuty membro, quando avvii una scansione antimalware su richiesta per le tue istanze Amazon EC2, potresti ricevere un errore. Puoi connetterti all'account di gestione per capire il motivo per cui è stata configurata una SCP per il tuo account membro. Per ulteriori informazioni, consulta [Effetti delle SCP sulle autorizzazioni](#).

Nuova scansione dell'istanza Amazon EC2 precedentemente scansionata

Indipendentemente dal fatto che una scansione venga GuardDuty avviata o avviata su richiesta, puoi avviare una nuova scansione antimalware su richiesta sulla stessa istanza Amazon EC2 dopo 1 ora dall'inizio della scansione malware precedente. Se la nuova scansione antimalware viene avviata entro 1 ora dall'avvio della scansione antimalware precedente, la richiesta genererà il seguente errore e non verrà generato alcun ID di scansione per questa richiesta.

```
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.
```

I passaggi per ripetere la scansione dell'istanza rimangono gli stessi dell'avvio di una scansione antimalware su richiesta per la prima volta. Per informazioni sui passaggi, consulta [Avvia la scansione antimalware su richiesta](#)

Per monitorare lo stato delle scansioni malware, consulta [Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for EC2](#).

Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for EC2

Dopo l'avvio di una scansione antimalware su un'istanza Amazon EC2 GuardDuty , fornisce automaticamente i campi di stato e risultato. Puoi monitorare lo stato attraverso le transizioni e vedere se è stato rilevato malware. La tabella seguente fornisce i possibili valori associati alla scansione antimalware.

Valori potenziali

Running, Completed Skipped, o Failed

Clean o Infected

GuardDuty initiated o On demand

*Il risultato della scansione viene compilato solo quando lo stato della scansione diventa Completed. Il risultato della scansione Infected indica che è GuardDuty stata rilevata la presenza di malware.

I risultati di ogni scansione malware vengono conservati per 90 giorni. Scegli il metodo di accesso che preferisci per monitorare lo stato della scansione malware.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Scansioni antimalware EC2.
3. Puoi filtrare le scansioni di malware in base alle seguenti proprietà disponibili nella barra di ricerca del filtro.
 - Scan ID: identificatore univoco associato alla scansione antimalware EC2.
 - ID account: Account AWS ID da cui è stata avviata la scansione del malware.
 - ARN dell'istanza EC2: Amazon Resource Name (ARN) associato all'istanza Amazon EC2 associata alla scansione.
 - Stato della scansione: lo stato di scansione del volume EBS, ad esempio in esecuzione, ignorato e completato
 - Tipo di scansione: indica se si tratta di una scansione antimalware su richiesta o di una GuardDuty scansione antimalware avviata.

API/CLI

- Dopo che la scansione antimalware ha prodotto un risultato di scansione, [DescribeMalwareScans](#) utilizzala per filtrare le scansioni antimalware sulla base di EC2_INSTANCE_ARN,,, SCAN_IDACCOUNT_ID, SCAN_TYPE GUARDDUTY_FINDING_ID e. SCAN_STATUS SCAN_START_TIME

I criteri di GUARDDUTY_FINDING_ID filtro sono disponibili quando SCAN_TYPE viene GuardDuty avviato.

- È possibile modificare l'esempio *filter-criteria* nel comando seguente. Attualmente, puoi applicare filtri utilizzando una CriterionKey alla volta. Le opzioni per la CriterionKey sono EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE GUARDDUTY_FINDING_ID, SCAN_STATUS e SCAN_START_TIME.

È possibile modificare *max-results* (fino a 50) e *sort-criteria*. Il AttributeName è obbligatorio e deve essere scanStartTime.

Nell'esempio seguente, i valori in *red* sono segnaposto. Sostituiscili con i valori appropriati per il tuo account. Ad esempio, sostituisci l'esempio detector-id *60b8777933648562554d637e0e4bb3b2* con il tuo validodetector-id. Se usi lo stesso di

CriterionKey seguito, assicurati di sostituire l'esempio EqualsValue con il tuo valido 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 risposta di questo comando mostra al massimo un risultato contenente i dettagli sulla risorsa interessata e sugli esiti relativi ai malware (se Infected).

GuardDuty account di servizio di Regione AWS

Quando un'istanza viene creata e condivisa con un account di GuardDuty servizio, nei CloudTrail registri viene creato un nuovo evento. Questo evento specifica l'snapshotId and userId (account di GuardDuty servizio corrispondente). Regione AWS Per ulteriori informazioni, consulta [In che modo GuardDuty esegue la scansione dei volumi EBS per il rilevamento di malware](#).

L'esempio seguente è un frammento di un CloudTrail evento che mostra il corpo della richiesta: ModifySnapshotAttribute

```
"requestParameters": {
  "snapshotId": "snap-1234567890abcdef0",
  "createVolumePermission": {
    "add": {
      "items": [
        {
          "userId": "111122223333"
        }
      ]
    }
  },
  "attributeType": "CREATE_VOLUME_PERMISSION"
}
```

La tabella seguente mostra gli account GuardDuty di servizio per ogni regione. userId È l'account del GuardDuty servizio e dipende dalla regione selezionata.

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (userId)
Stati Uniti orientali (Virginia settentrionale)	us-east-1	652050842985
Stati Uniti orientali (Ohio)	us-east-2	178123968615
Stati Uniti occidentali (California settentrionale)	us-west-1	669213148797
Stati Uniti occidentali (Oregon)	us-west-2	447226417196
Asia Pacifico (Mumbai)	ap-south-1	913179291432
Asia Pacifico (Osaka)	ap-northeast-3	089661699081
Asia Pacifico (Seul)	ap-northeast-2	039163547507
Asia Pacifico (Tokyo)	ap-northeast-1	874749492622
Asia Pacifico (Singapore)	ap-southeast-1	247460962669
Asia Pacifico (Sydney)	ap-southeast-2	124839743349
Canada (Centrale)	ca-central-1	175877067165
Canada occidentale (Calgary)	ca-west-1	894794104037
Europa (Francoforte)	eu-central-1	002294850712
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londra)	eu-west-2	310125036783
Europa (Parigi)	eu-west-3	866607715269
Europa (Stoccolma)	eu-north-1	693780578038

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (userId)
Cina (Pechino)	cn-north-1	448721096076
Cina (Ningxia)	cn-northwest-1	480864352451
Sud America (San Paolo)	sa-east-1	546914126324
Asia Pacifico (Hyderabad) (con consenso esplicito)	ap-south-2	682251015962
Asia Pacifico (Melbourne) (con consenso esplicito)	ap-southeast-4	353488359550
Asia Pacifico (Malesia) (Opt-in)	ap-southeast-5	009160069308
Asia Pacifico (Tailandia) (Opt-in)	ap-southeast-7	941377115582
Europa (Spagna) (con consenso esplicito)	eu-south-2	936182149045
Europa (Zurigo) (con consenso esplicito)	eu-central-2	867642063380
Israele (Tel Aviv) (con consenso esplicito)	il-central-1	619233833001
Europa (Milano) (con consenso esplicito)	eu-south-1	977238331021
Asia Pacifico (Hong Kong) (con consenso esplicito)	ap-east-1	249472122084
Medio Oriente (Bahrein) (con consenso esplicito)	me-south-1	404001805210

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (userId)
Africa (Città del Capo) (con consenso esplicito)	af-south-1	957664736811
Asia Pacifico (Giacarta) (con consenso esplicito)	ap-southeast-3	452118225523
Medio Oriente (EAU) (con consenso esplicito)	me-central-1	828603743433
Messico (Centrale) (Opt- in)	mx-central-1	557690616787
Asia Pacifico (Taipei)	ap-east-2	863518437308
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	686255982852
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	226283551151
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	226300430612

Quote nella protezione da malware per EC2

Questa sezione include le quote associate all'utilizzo di Malware Protection for EC2. Per le quote associate GuardDuty a, vedi. [GuardDuty quote](#)

La tabella seguente fornisce la disponibilità predefinita di varie risorse quando si utilizza Malware Protection for EC2.

Scope	Predefinita	Commenti
Estrazione e analisi dei dati in file compressi o archiviati	5	Il numero massimo di livelli nidificati consentiti in un file archiviato.
Numero di file all'interno di un file archiviato	1000	Il numero massimo di file che possono essere scansati all'interno di un archivio. Questo conteggio è la somma del numero di file estratti dall'archivio e del numero di file estratti da tutti gli archivi annidati.
Numero delle minacce	32	Il numero massimo di minacce che è possibile visualizzare nel pannello dei risultati. GuardDuty Malware Protection for EC2 potrebbe aver rilevato più nomi di minacce. Se il numero di nomi di minacce rilevate è superiore al valore predefinito, puoi visualizzare i dettagli JSON selezionando il Finding ID sotto il nome del risultato nel pannello dei dettagli della GuardDuty console.
Numero di file per minaccia rilevata	5	Il numero massimo di file identificati per ogni minaccia rilevata. Ad esempio, se GuardDuty rileva 10 file associati a una singola minaccia, la minaccia mostrerà un massimo di 5 file.

Scope	Predefinita	Commenti
Volumi EBS per ogni scansione di ogni istanza	11	Il numero massimo di volumi EBS che GuardDuty possono essere scansionati per istanza EC2. Se ci sono più di 11 volumi EBS da scansionare, GuardDuty Malware Protection for EC2 li ordina <code>deviceName</code> alfabeticamente e seleziona i primi 11 volumi EBS.
Dimensione del volume EBS	2048 GB	Associato a un'istanza Amazon EC2 e a un carico di lavoro di container, GuardDuty Malware Protection for EC2 può scansionare ogni volume Amazon EBS di dimensioni fino a 2048 GB. Questa quota si applica a tutti i paesi Regione AWS in cui è disponibile il supporto per Malware Protection for EC2.

Scope	Predefinita	Commenti
Tipi di file system supportati	GuardDuty Malware Protection for EC2 può scansionare i seguenti tipi di file system: • New Technology File System (NTFS) • X File System (XFS) • File System second extended (ext2) • File System fourth extended (ext4) • File system File Allocation Table (FAT) • File system Virtual File Allocation Table (VFAT)	N/D.
Tag delle opzioni di scansione	50	Il numero massimo dei tag delle risorse che puoi aggiungere per personalizzare l'impostazione delle opzioni di scansione malware. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente .
Ritrovamento del periodo di conservazione	90	Il numero massimo di giorni in cui viene GuardDuty conservato un risultato. Per le informazioni più recenti, consulta GuardDuty Quote Amazon .

Scope	Predefinita	Commenti
Periodo di conservazione delle scansioni malware	90	Il numero massimo di giorni in cui GuardDuty Malware Protection for EC2 conserva la cronologia di una scansione. Per ulteriori informazioni sulla visualizzazione delle scansioni malware recenti, consulta Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for EC2 .
Transazioni al secondo (TPS) per la scansione antimalware on demand	1	Il numero di richieste di scansione antimalware on demand che possono essere avviate al secondo in ciascuna regione.
Limite di burst per la scansione antimalware on demand	1	Il numero di richieste simultanee di scansione antimalware on demand che possono essere avviate al secondo in ciascuna regione.

GuardDuty Protezione da malware per S3

Malware Protection for S3 ti aiuta a rilevare la potenziale presenza di malware scansionando gli oggetti appena caricati nel bucket Amazon Simple Storage Service (Amazon S3) selezionato. Quando un oggetto S3 o una nuova versione di un oggetto S3 esistente viene caricato nel bucket selezionato, GuardDuty avvia automaticamente una scansione antimalware.

[Protezione da malware per S3: panoramica e demo](#)

Due approcci per abilitare la protezione da malware per S3

Puoi abilitare Malware Protection for S3 quando attivi il GuardDuty servizio e utilizzi Malware Protection for S3 come parte dell' GuardDuty esperienza complessiva, oppure quando desideri utilizzare la funzionalità Malware Protection for S3 da sola senza abilitare il servizio. Account AWS GuardDuty Quando attivi da sola Malware Protection for S3, nella GuardDuty documentazione si fa riferimento all'utilizzo di Malware Protection for S3 come funzionalità indipendente.

Considerazioni sull'utilizzo indipendente di Malware Protection for S3

- GuardDuty risultati di sicurezza: Detector ID è un identificatore univoco associato al tuo account in una regione. Quando abiliti GuardDuty in una o più regioni in un account, viene creato automaticamente un ID rilevatore per questo account in ogni regione in cui attivi. GuardDuty

Per ulteriori informazioni, consulta Detector nel [Concetti e termini chiave in Amazon GuardDuty](#) documento.

Quando abiliti Malware Protection for S3 in modo indipendente in un account, a quell'account non sarà associato un ID rilevatore. Ciò influisce sulle GuardDuty funzionalità che potresti avere a tua disposizione. Ad esempio, quando una scansione antimalware di S3 rileva la presenza di malware, non viene generato alcun GuardDuty risultato Account AWS perché tutti i GuardDuty risultati sono associati a un ID del rilevatore.

- Verifica se l'oggetto scansionato è dannoso: per impostazione predefinita, GuardDuty pubblica i risultati della scansione del malware sul bus di EventBridge eventi Amazon predefinito e su un namespace Amazon CloudWatch . Quando abiliti il tagging al momento dell'attivazione di Malware Protection for S3 per un bucket, l'oggetto S3 scansionato riceve un tag che riporta il risultato della scansione. Per ulteriori informazioni sull'assegnazione di tag, consulta [Etichettatura opzionale degli oggetti in base al risultato della scansione](#).

Considerazioni generali per abilitare Malware Protection for S3

Le seguenti considerazioni generali valgono sia che si utilizzi Malware Protection for S3 in modo indipendente o come parte dell'esperienza: GuardDuty

- Puoi abilitare Malware Protection for S3 per un bucket Amazon S3 che appartiene al tuo account. Come account GuardDuty amministratore delegato non puoi abilitare questa funzionalità in un bucket Amazon S3 che appartiene a un account membro.
- Puoi abilitare questa funzionalità nei bucket S3 che appartengono alla stessa regione attualmente selezionata nella console. GuardDuty non supporta l'attivazione di questa funzionalità nei bucket S3 interregionali.
- In qualità di account GuardDuty amministratore delegato, riceverai una EventBridge notifica Amazon ogni volta che si verifica una modifica in un bucket S3 che uno [Visualizzazione e comprensione dello stato del bucket protetto](#) degli account membri della tua organizzazione ha configurato per questa funzionalità.

Indice

- [Prezzi e costi di utilizzo di Malware Protection for S3](#)
- [Come funziona Malware Protection for S3?](#)
- [Funzionalità di protezione da malware per S3](#)
- [\(Facoltativo\) Inizia a usare GuardDuty Malware Protection for S3 in modo indipendente \(solo console\)](#)

- [Configurazione della protezione da malware per S3 per il tuo bucket](#)
- [Passaggi dopo l'attivazione di Malware Protection for S3](#)
- [Scansione malware su richiesta per S3 GuardDuty](#)
- [Utilizzo del controllo degli accessi basato su tag \(TBAC\) con Malware Protection for S3](#)
- [Visualizzazione e comprensione dello stato del bucket protetto](#)
- [Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3](#)
- [Risoluzione dei problemi](#)
- [Modifica del piano di protezione da malware per un bucket protetto](#)
- [Disattivazione di Malware Protection for S3 per un bucket protetto](#)
- [Supportabilità delle funzionalità di Amazon S3](#)
- [Quote nella protezione da malware per S3](#)

Prezzi e costi di utilizzo di Malware Protection for S3

I prezzi di Malware Protection for S3 funzionano in modo diverso rispetto ad altri piani di protezione di GuardDuty. Mentre la maggior parte dei piani di GuardDuty protezione prevede una prova gratuita a breve termine di 30 giorni, Malware Protection for S3 segue il piano Free Tier di 12 mesi. AWS Per informazioni sui GuardDuty prezzi, consulta [Prezzi in GuardDuty](#).

L'elenco seguente fornisce i costi di prezzo associati all'utilizzo di Malware Protection for S3.

Piano di livello gratuito (costo di scansione)

Ciascuno Account AWS riceve un piano gratuito di 12 mesi che include l'utilizzo fino a un limite mensile specifico per ciascuna regione. Ciascuno Account AWS riceve un piano gratuito mensile di utilizzo fino a 1.000 richieste e 1 GB di dati scansionati. Se l'utilizzo supera il limite specificato, inizierai a sostenere il costo di utilizzo per il limite superato. Per i dettagli completi sui prezzi, consulta i prezzi dei piani di [GuardDuty protezione](#).

Important

La scansione su richiesta non è inclusa nel piano gratuito.

Per informazioni sul costo di utilizzo dopo l'attivazione di Malware Protection for S3, consulta [Analisi dei costi di utilizzo di Malware Protection for S3](#).

Costo di utilizzo di S3 Object Tagging

Quando abiliti Malware Protection for S3, è facoltativo abilitare i tag per gli oggetti S3 scansionati. Quando scegli di abilitare S3 Object Tagging, è associato un costo di utilizzo. Per ulteriori informazioni sui costi, consulta la [scheda Management & Insights nella pagina](#) dei prezzi di Amazon S3.

Il costo di utilizzo di S3 Object Tagging non è incluso nel piano Free Tier.

Amazon S3 APIs GET e PUT costi di utilizzo

L' GuardDuty esecuzione di Amazon APIs S3 in base al ruolo IAM comporta costi di utilizzo. Ad esempio, dopo aver assunto il ruolo IAM, GuardDuty esegue l'PutObjectAPI per aggiungere l'oggetto di test al bucket selezionato. Questo aiuta a GuardDuty valutare lo stato di attivazione della funzionalità.

Per informazioni sui prezzi delle chiamate API S3 nella tua Regione AWS, consulta [Richieste e recupero dati nella scheda Storage e richieste nella pagina](#) dei prezzi di Amazon S3.

Analisi dei costi di utilizzo di Malware Protection for S3

Il tuo account inizia a sostenere costi di utilizzo quando utilizzi Malware Protection for S3 oltre il limite specifico del piano Free Tier o quando scade il piano Free Tier di 12 mesi del tuo account. Per informazioni sul piano Free Tier, consulta. [Prezzi e costi di utilizzo di Malware Protection for S3](#) Tieni presente che il piano gratuito non si applica alla scansione su richiesta di oggetti Malware Protection for S3.

La GuardDuty console non supporta la revisione dei costi di utilizzo di Malware Protection for S3. Per visualizzare il costo di utilizzo, accedi a Cost Explorer nella <https://console.aws.amazon.com/costmanagement/console>. Per informazioni sulla Account AWS fatturazione, consulta la [Guida per l'AWS Billing utente](#).

Per informazioni sul costo di utilizzo stimato in GuardDuty, vedere [Monitoraggio dell'utilizzo e stima dei costi](#).

Come funziona Malware Protection for S3?

Questa sezione descrive i componenti di Malware Protection for S3, come funziona dopo averlo abilitato per un bucket S3 e come esaminare lo stato e i risultati della scansione del malware.

Panoramica di

Puoi abilitare Malware Protection for S3 per un bucket Amazon S3 che appartiene al tuo Account AWS GuardDuty. Offre la flessibilità necessaria per abilitare questa funzionalità per l'intero bucket o limitare l'ambito della scansione antimaleware a [prefissi di oggetti specifici, in cui GuardDuty analizza ogni oggetto caricato che inizia con uno dei prefissi](#) selezionati. È possibile aggiungere fino a 5 prefissi. Quando abiliti la funzionalità per un bucket S3, quel bucket viene chiamato bucket protetto.

Autorizzazioni del ruolo IAM

Malware Protection for S3 utilizza un ruolo IAM che consente di eseguire le azioni di scansione del malware GuardDuty per tuo conto. Queste azioni includono la notifica dei nuovi oggetti caricati nel bucket selezionato, la scansione di tali oggetti e, facoltativamente, l'aggiunta di tag agli oggetti scansionati. Questo è un prerequisito per configurare il bucket S3 con questa funzionalità.

È possibile aggiornare un ruolo IAM esistente o creare un nuovo ruolo per questo scopo. Quando abiliti Malware Protection for S3 per più di un bucket, puoi aggiornare il ruolo IAM esistente per includere il nome dell'altro bucket, se necessario. Per ulteriori informazioni, consulta [Creare o aggiornare la politica dei ruoli IAM](#).

Etichettatura opzionale degli oggetti in base al risultato della scansione

Al momento di abilitare Malware Protection for S3 per il tuo bucket, è disponibile un passaggio opzionale per abilitare l'etichettatura per gli oggetti S3 scansionati. Il ruolo IAM include già l'autorizzazione ad aggiungere tag all'oggetto dopo la scansione. Tuttavia, GuardDuty aggiungerà tag solo quando abiliti questa opzione al momento della configurazione.

È necessario abilitare questa opzione prima che un oggetto venga caricato. Al termine della scansione, GuardDuty aggiunge un tag predefinito all'oggetto S3 scansionato con la seguente coppia chiave:valore:

GuardDutyMalwareScanStatus:*Potential scan result*

I potenziali valori dei tag dei risultati della scansione includono NO_THREATS_FOUND,,, e THREATS_FOUND. UNSUPPORTED ACCESS_DENIED FAILED Per ulteriori informazioni su questi valori, consulta [the section called “Potenziale stato di scansione dell'oggetto S3 e stato dei risultati”](#).

L'abilitazione dei tag è uno dei modi per conoscere i risultati della scansione degli oggetti S3. Puoi utilizzare ulteriormente questi tag per aggiungere una politica delle risorse S3 di controllo degli

accessi basata su tag (TBAC) in modo da poter intraprendere azioni sugli oggetti potenzialmente dannosi. Per ulteriori informazioni, consulta [Aggiungere TBAC alla risorsa bucket S3](#).

Ti consigliamo di abilitare i tag al momento della configurazione di Malware Protection for S3 per il tuo bucket. Se abiliti l'etichettatura dopo il caricamento di un oggetto e potenzialmente l'avvio della scansione, non GuardDuty sarà possibile aggiungere tag all'oggetto scansionato. Per informazioni sui costi associati all'etichettatura degli oggetti S3, consulta [Prezzi e costi di utilizzo di Malware Protection for S3](#)

Procedura dopo aver abilitato Malware Protection for S3 per un bucket

Dopo aver abilitato Malware Protection for S3, viene creata una risorsa del piano Malware Protection esclusivamente per il bucket S3 selezionato. Questa risorsa è associata a un ID del piano Malware Protection, un identificatore univoco per la risorsa protetta. Utilizzando una delle autorizzazioni IAM GuardDuty, crea e gestisce una regola EventBridge gestita denominata `D0-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

Come GuardDuty gestisce i tuoi dati: guardrails per la protezione dei dati

Malware Protection for S3 ascolta le notifiche di Amazon EventBridge. Quando un oggetto viene caricato nel bucket selezionato o in uno dei prefissi, GuardDuty scarica quell'oggetto dal bucket S3 utilizzando un bucket, quindi lo legge, lo decrittografa [AWS PrivateLink](#) e scansiona in un ambiente isolato nella stessa regione. L'ambiente di scansione viene eseguito in un cloud privato virtuale (VPC) bloccato senza accesso a Internet. Il VPC è collegato a un gruppo di regole DNS Firewall che consente la comunicazione solo con i domini consentiti elencati di cui è proprietario. AWS [Per tutta la durata della scansione, memorizza GuardDuty temporaneamente l'oggetto S3 scaricato all'interno dell'ambiente di scansione crittografato con chiavi \(\).](#)[AWS Key Management Service](#)[AWS KMS](#)

Note

Per impostazione predefinita, tutti gli Amazon S3 APIs elencati nel [tipo Object Created Event](#) nella Amazon S3 User Guide avvieranno la scansione Malware Protection for S3.

Questi tipi di eventi includono [PutObjectPOST Object](#) e [CopyObjectCompleteMultipartUpload](#)

Per informazioni sulla metodologia di rilevamento del GuardDuty malware e sui motori di scansione utilizzati, consulta [GuardDuty motore di scansione per il rilevamento di malware](#).

Al termine della scansione antimalware, GuardDuty elabora i metadati di scansione con lo stato della scansione e quindi elimina la copia scaricata dell'oggetto.

GuardDuty pulisce l'ambiente di scansione ogni volta prima che inizi una nuova scansione.

GuardDuty utilizza l'autorizzazione contingente per l'accesso dell'operatore all'ambiente di scansione e ogni richiesta di accesso viene esaminata, approvata e verificata.

Revisione dello stato e dei risultati della scansione degli oggetti S3

GuardDuty pubblica l'evento del risultato della scansione degli oggetti S3 sul bus eventi EventBridge predefinito di Amazon. GuardDuty invia anche i parametri di scansione, come il numero di oggetti scansionati e i byte scansionati, ad Amazon CloudWatch. Se hai abilitato l'etichettatura, GuardDuty aggiungerà il tag predefinito `GuardDutyMalwareScanStatus` e un potenziale risultato della scansione come valore del tag.

Important

GuardDuty utilizza at-least-once la consegna, il che significa che potresti ricevere più risultati di scansione per lo stesso oggetto. Consigliamo di progettare le applicazioni per gestire risultati duplicati. Ti viene addebitata una sola volta per ogni oggetto scansionato.

Per ulteriori informazioni, consulta [Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3](#).

Revisione dei risultati generati

La revisione dei risultati dipende dal fatto che tu stia utilizzando o meno Malware Protection for S3 con GuardDuty. Considerare i seguenti scenari:

Utilizzo di Malware Protection for S3 quando il GuardDuty servizio è abilitato (detector ID)

Se la scansione antimalware rileva un file potenzialmente dannoso in un oggetto S3, GuardDuty genererà un risultato associato. È possibile visualizzare i dettagli del risultato e utilizzare i passaggi consigliati per correggere potenzialmente il risultato. In base alla [frequenza di esportazione dei risultati](#), i risultati generati vengono esportati in un bucket S3 e in un bus di eventi. EventBridge

Per informazioni sul tipo di risultato che verrebbe generato, consulta [Protezione da malware per tipo di ricerca S3](#)

Utilizzo di Malware Protection for S3 come funzionalità indipendente (nessun ID di rilevamento)

GuardDuty non sarà in grado di generare risultati perché non esiste un ID del rilevatore associato. Per conoscere lo stato della scansione antimalware degli oggetti S3, puoi visualizzare il risultato della scansione che GuardDuty viene pubblicato automaticamente sul tuo bus eventi predefinito. Puoi anche visualizzare le CloudWatch metriche per valutare il numero di oggetti e byte che GuardDuty hanno tentato di scansionare. È possibile impostare CloudWatch allarmi per ricevere notifiche sui risultati della scansione. Se hai abilitato S3 Object Tagging, puoi anche visualizzare lo stato della scansione antimalware controllando l'oggetto S3 per la chiave del tag e il valore del GuardDutyMalwareScanStatus tag dei risultati della scansione.

Per informazioni sullo stato e sui risultati della scansione degli oggetti S3, consulta [Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3](#)

Funzionalità di protezione da malware per S3

L'elenco seguente fornisce una panoramica di ciò che puoi aspettarti o fare dopo aver abilitato Malware Protection for S3 per il tuo bucket:

- Scegli cosa scansionare: scansiona i file man mano che vengono caricati su tutti i prefissi o su alcuni prefissi specifici (fino a 5) associati al bucket S3 selezionato.
- Scansioni automatiche degli oggetti caricati: dopo aver abilitato Malware Protection for S3 per un bucket, GuardDuty avvierà automaticamente una scansione per rilevare potenziali malware in un oggetto appena caricato.
- Scansioni su richiesta: è possibile avviare scansioni per oggetti esistenti o scansionare nuovamente gli oggetti precedentemente scansionati. Per ulteriori informazioni, consulta [Scansione malware su richiesta per S3 GuardDuty](#).
- Abilita tramite console, utilizzando API/AWS CLI oppure CloudFormation: scegli un metodo preferito per abilitare Malware Protection for S3.

Puoi abilitare Malware Protection for S3 utilizzando piattaforme Infrastructure as code (IaC) come Terraform. [Per ulteriori informazioni, consulta Resource: aws_guardduty_malware_protection_plan](#)

- Formati di file supportati, quote Malware Protection per S3 e funzionalità di Amazon S3: Malware Protection for S3 supporta tutti i formati di file che puoi caricare in un bucket S3. Se il file caricato è protetto da password ed GuardDuty è in grado di rilevare la presenza di una protezione tramite password per il tipo di file caricato, GuardDuty tenterà di scansionare il contenuto originale

utilizzando password comuni. Se la password fallisce, la scansione verrà ignorata. GuardDuty non riesce a rilevare la presenza della protezione tramite password su tutti i formati di file. Se non GuardDuty riesce a rilevare la presenza della protezione tramite password, GuardDuty eseguirà comunque la scansione del contenuto crittografato.

Per informazioni sulle quote relative alla dimensione degli oggetti, al livello massimo di profondità di archiviazione e ad altri dettagli, vedere [Quote nella protezione da malware per S3](#).

Per informazioni sul supporto o meno di una funzionalità di Amazon S3, consulta [Supportabilità delle funzionalità di Amazon S3](#)

- Supporta l'etichettatura degli oggetti S3 scansionati: se abiliti [Etichettatura opzionale degli oggetti in base al risultato della scansione](#), dopo ogni scansione antimalware, GuardDuty aggiungerà un tag che indica lo stato della scansione. Puoi utilizzare questo tag per configurare il controllo degli accessi basato su tag (TBAC) per gli oggetti S3. Ad esempio, puoi limitare l'accesso agli oggetti S3 che sono indicati come dannosi e che hanno il valore del tag come. THREATS_FOUND
- EventBridge Notifiche Amazon: GuardDuty invia eventi ad Amazon EventBridge quando lo stato delle risorse del piano Malware Protection cambia o viene completata una scansione antimalware dell'oggetto S3. Questi eventi vengono inviati al bus degli eventi predefinito. È possibile utilizzare EventBridge e questi eventi per scrivere regole che intraprendono azioni, come il monitoraggio del verificarsi di questi eventi. Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#).
- CloudWatch metriche: visualizza le CloudWatch metriche per abilitare gli allarmi su determinati stati di scansione del malware. Per ulteriori informazioni, consulta [Metriche dello stato di scansione degli oggetti S3 in CloudWatch](#).

(Facoltativo) Inizia a usare GuardDuty Malware Protection for S3 in modo indipendente (solo console)

Utilizza questo passaggio facoltativo per iniziare a utilizzare l'opzione di rilevamento delle minacce di Malware Protection for S3 indipendentemente GuardDuty dallo stato del tuo Account AWS

Se desideri utilizzare anche altri piani di protezione dedicati GuardDuty, devi iniziare con il GuardDuty servizio Amazon. Per informazioni sui piani di GuardDuty protezione, consulta [Caratteristiche di GuardDuty](#). Se l'hai già abilitato GuardDuty nel tuo account, puoi saltare questo passaggio e continuare. [Configurazione della protezione da malware per S3 per il tuo bucket](#)

Passaggi per iniziare a utilizzare solo il rilevamento delle minacce da parte di Malware Protection for S3

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Seleziona GuardDuty Malware Protection solo per S3. Questo ti aiuta a rilevare se un file appena caricato nel tuo bucket Amazon Simple Storage Service (Amazon S3) contiene potenzialmente malware.

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. Scegli Avvia. Ora puoi continuare con i passaggi indicati [Configurazione della protezione da malware per S3 per il tuo bucket](#) di seguito.

Configurazione della protezione da malware per S3 per il tuo bucket

Affinché Malware Protection for S3 esegua la scansione e (facoltativamente) aggiunga tag agli oggetti S3, puoi utilizzare ruoli di servizio che dispongono delle autorizzazioni necessarie per eseguire azioni

di scansione del malware per tuo conto. [Per ulteriori informazioni sull'utilizzo dei ruoli di servizio per abilitare la protezione da malware per S3, consulta Service Access.](#) Questo ruolo è diverso dal ruolo collegato al [servizio GuardDuty Malware Protection](#).

Se preferisci utilizzare i ruoli IAM, puoi associare un ruolo IAM che include le autorizzazioni necessarie per eseguire la scansione e (facoltativamente) aggiungere tag agli oggetti S3. GuardDuty assume quindi questo ruolo IAM per eseguire queste azioni per tuo conto. Avrai bisogno di questo nome di ruolo IAM al momento dell'attivazione di questo piano di protezione per il tuo bucket Amazon S3.

Se utilizzi ruoli IAM, per ogni volta che desideri proteggere un bucket Amazon S3, devi eseguire entrambi i passaggi elencati in questa sezione.

Per abilitare Malware Protection for S3, avrai bisogno di dettagli come il nome del bucket S3, i prefissi degli oggetti se desideri concentrare la protezione per prefissi specifici e il nome del ruolo IAM con le autorizzazioni richieste.

I passaggi rimangono invariati sia che tu inizi a usare Malware Protection for S3 in modo indipendente sia che lo abiliti come parte del servizio. GuardDuty

Argomenti

1. [Creare o aggiornare la politica dei ruoli IAM](#)
2. [Attivazione della protezione da malware per S3 per il tuo bucket](#)
3. [Risoluzione dell'errore relativo alle autorizzazioni dei ruoli IAM](#)

Attivazione della protezione da malware per S3 per il tuo bucket

Questa sezione fornisce passaggi dettagliati su come abilitare Malware Protection for S3 per un bucket nel tuo account. Prima di procedere, esamina le seguenti considerazioni:

- Quando abiliti questo piano di protezione utilizzando la GuardDuty console, include il passaggio per creare un nuovo ruolo o utilizzare un ruolo esistente nella sezione Accesso al servizio.
- Quando abiliti questo piano di protezione utilizzando l' GuardDuty API o la CLI, devi [Creare o aggiornare la politica dei ruoli IAM](#) prima procedere ulteriormente.
- Indipendentemente dal modo in cui si abilita questo piano di protezione, è necessario disporre del necessario. [Autorizzazioni per creare una risorsa del piano Malware Protection](#)

Considerando la limitazione del bucket Amazon S3

S3 Throttling potrebbe limitare la velocità con cui i dati possono essere trasferiti da o verso i bucket Amazon S3. Ciò può potenzialmente ritardare le scansioni antimalware degli oggetti appena caricati.

Se ti aspetti volumi GET e PUT richieste elevati verso i tuoi bucket S3, prendi in considerazione l'implementazione di misure per prevenire il throttling. Per informazioni su come eseguire questa operazione, consulta [Prevent Amazon S3 throttling](#) nella Guida per l'utente di Amazon Athena.

Autorizzazioni per creare una risorsa del piano Malware Protection

Quando abiliti Malware Protection for S3 per un bucket Amazon S3 GuardDuty , crea una risorsa del piano Malware Protection che funge da identificatore per il piano di protezione del bucket. Se non stai già utilizzando [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#), devi aggiungere le seguenti autorizzazioni per creare questa risorsa:

- guardDuty:CreateMalwareProtectionPlan
- iam:PassRole

Puoi utilizzare il seguente esempio di politica personalizzata e sostituirla *placeholder values* con i valori appropriati per il tuo account:

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": "*"   
    }  
]  
}
```

Attivazione della protezione da malware per S3 tramite console GuardDuty

Le seguenti sezioni forniscono una step-by-step guida dettagliata, come speriementerai nella console GuardDuty

Per abilitare Malware Protection for S3 utilizzando la console GuardDuty

Inserisci i dettagli del bucket S3

Utilizza i seguenti passaggi per fornire i dettagli del bucket Amazon S3:

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri abilitare Malware Protection for S3.
3. Nel pannello di navigazione, scegli Malware Protection for S3.
4. Nella sezione Bucket protetti, scegli Abilita per abilitare la protezione da malware per S3 per un bucket S3 che appartiene al tuo Account AWS
5. In Inserisci i dettagli del bucket S3, inserisci il nome del bucket Amazon S3. In alternativa, scegli Browse S3 per selezionare un bucket S3.

Il Regione AWS bucket S3 e il Account AWS punto in cui abiliti Malware Protection for S3 devono coincidere. Ad esempio, se il tuo account appartiene alla us-east-1 regione, deve esserlo anche la tua regione del bucket Amazon S3. us-east-1

6. In Prefisso, puoi selezionare Tutti gli oggetti nel bucket S3 o Oggetti che iniziano con un prefisso specifico.

- Seleziona Tutti gli oggetti nel bucket S3 quando vuoi GuardDuty puoi scansionare tutti gli oggetti appena caricati nel bucket selezionato.
- Seleziona Oggetti che iniziano con un prefisso specifico quando desideri scansionare gli oggetti appena caricati che appartengono a un prefisso specifico. Questa opzione consente di concentrare l'ambito della scansione antimalware solo sui prefissi degli oggetti selezionati. Per ulteriori informazioni sull'uso dei prefissi, consulta [Organizzazione degli oggetti nella console Amazon S3 utilizzando](#) le cartelle nella Amazon S3 User Guide.

Scegli Aggiungi prefisso e inserisci il prefisso. Puoi aggiungere fino a cinque prefissi.

Abilita l'etichettatura per gli oggetti scansionati

Si tratta di un passaggio facoltativo. Quando abiliti l'opzione di etichettatura prima che un oggetto venga caricato nel tuo bucket, dopo aver completato la scansione, GuardDuty aggiungerà un tag predefinito con chiave `as GuardDutyMalwareScanStatus` e il valore come risultato della scansione. Per utilizzare Malware Protection for S3 in modo ottimale, consigliamo di abilitare l'opzione per aggiungere tag agli oggetti S3 al termine della scansione. Si applica il costo standard di S3 Object Tagging. Per ulteriori informazioni, consulta [Prezzi e costi di utilizzo di Malware Protection for S3](#).

Perché dovresti abilitare il tagging?

- L'attivazione dei tag è uno dei modi per conoscere i risultati della scansione antimalware. Per informazioni sui risultati di una scansione antimalware S3, consulta [Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3](#)
- Configura una politica di controllo degli accessi basata su tag (TBAC) sul tuo bucket S3 che contiene l'oggetto potenzialmente dannoso. Per informazioni sulle considerazioni e su come implementare il controllo degli accessi basato su tag (TBAC), consulta [Utilizzo del controllo degli accessi basato su tag \(TBAC\) con Malware Protection for S3](#)

Considerazioni sull'aggiunta di un tag GuardDuty all'oggetto S3:

- Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto. Per ulteriori informazioni, consulta [Categorizzazione dello storage mediante tag nella Guida](#) per l'utente di Amazon S3.

Se tutti e 10 i tag sono già in uso, non è GuardDuty possibile aggiungere il tag predefinito all'oggetto scansionato. GuardDuty pubblica inoltre il risultato della scansione nel bus degli eventi

predefinito EventBridge . Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#).

- Se il ruolo IAM selezionato non include l'autorizzazione GuardDuty per taggare l'oggetto S3, anche con l'etichettatura abilitata per il bucket protetto, non GuardDuty sarà possibile aggiungere tag a questo oggetto S3 scansionato. Per ulteriori informazioni sull'autorizzazione del ruolo IAM richiesta per l'etichettatura, consulta. [Creare o aggiornare la politica dei ruoli IAM](#)

GuardDuty pubblica inoltre il risultato della scansione nel bus EventBridge degli eventi predefinito. Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#).

Per selezionare un'opzione in Etichetta gli oggetti scansionati

- GuardDuty Per aggiungere tag agli oggetti S3 scansionati, seleziona Etichetta gli oggetti.
- Se non desideri aggiungere tag GuardDuty agli oggetti S3 scansionati, seleziona Non etichettare gli oggetti.

Accesso al servizio

Utilizza i seguenti passaggi per scegliere un ruolo di servizio esistente o creare un nuovo ruolo di servizio con le autorizzazioni necessarie per eseguire azioni di scansione antimalware per tuo conto. Queste azioni possono includere la scansione degli oggetti S3 appena caricati e (facoltativamente) l'aggiunta di tag a tali oggetti. Per informazioni sulle autorizzazioni che avrà questo ruolo, consulta. [Creare o aggiornare la politica dei ruoli IAM](#)

Nella sezione Accesso al servizio, puoi effettuare una delle seguenti operazioni:

1. Creare e utilizzare un nuovo ruolo di servizio: è possibile utilizzare la funzione Crea un nuovo ruolo di servizio con le autorizzazioni necessarie per eseguire la scansione antimalware.

Sotto il nome del ruolo puoi scegliere di utilizzare il nome precompilato da GuardDuty o inserire un nome significativo a tua scelta per identificare il ruolo. Ad esempio, GuardDutyS3MalwareScanRole. Il nome del ruolo deve contenere da 1 a 64 caratteri. I caratteri validi sono a-z, A-Z, 0-9 e '+', '@', '_', '-'.

2. Usa un ruolo di servizio esistente: puoi scegliere un ruolo di servizio esistente dall'elenco dei nomi del ruolo di servizio.

- a. In Modello di policy puoi visualizzare la policy per il tuo bucket S3. Assicurati di aver inserito o selezionato un bucket S3 nella sezione Inserisci i dettagli del bucket S3.
- b. In Nome del ruolo di servizio scegli un ruolo di servizio dall'elenco dei ruoli di servizio.

Puoi apportare modifiche alla policy in base ai tuoi requisiti. Per maggiori dettagli su come creare o aggiornare un ruolo IAM, consulta [Creare o aggiornare la policy del ruolo IAM](#).

Per problemi con le autorizzazioni dei ruoli IAM, consulta [Risoluzione dell'errore relativo alle autorizzazioni dei ruoli IAM](#).

(Facoltativo) Etichetta l'ID del piano di protezione da malware

Si tratta di un passaggio facoltativo che consente di aggiungere tag alla risorsa del piano Malware Protection che verrebbe creata per la risorsa del bucket S3.

Ogni tag è composto da due parti: una chiave di tag e un valore di tag opzionale. Per ulteriori informazioni sull'etichettatura e sui relativi vantaggi, consulta Risorse per l'[etichettatura AWS](#).

Per aggiungere tag alla risorsa del piano Malware Protection

1. Inserisci la chiave e un valore opzionale per il tag. Sia la chiave che il valore del tag fanno distinzione tra maiuscole e minuscole. Per informazioni sui nomi della chiave e del valore del tag, consulta [Limiti e requisiti di denominazione dei tag](#).
2. Per aggiungere altri tag alla risorsa del piano Malware Protection, scegli Aggiungi nuovo tag e ripeti il passaggio precedente. Puoi aggiungere fino a 50 tag per ciascuna risorsa .
3. Scegli Abilita .

Abilitazione della protezione da malware per S3 tramite API/CLI

Questa sezione include i passaggi da seguire quando si desidera abilitare Malware Protection for S3 a livello di codice nel proprio ambiente. AWS Ciò richiede il ruolo IAM Amazon Resource Name (ARN) che hai creato in questa fase -. [Creare o aggiornare la politica dei ruoli IAM](#)

Per abilitare la protezione da malware per S3 a livello di codice utilizzando API/CLI

- Utilizzando l'API

Esegui [CreateMalwareProtectionPlan](#) per abilitare Malware Protection for S3 per un bucket che appartiene al tuo account.

- Utilizzando AWS CLI

A seconda di come si desidera abilitare Malware Protection for S3, il seguente elenco fornisce comandi di AWS CLI esempio per casi d'uso specifici. Quando esegui questi comandi, sostituisci *placeholder examples shown in red*, con i valori appropriati per il tuo account.

AWS CLI comandi di esempio

- Utilizzate il seguente AWS CLI comando per abilitare Malware Protection for S3 per un bucket senza tag per gli oggetti S3 scansionati:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::111122223333:role/role-name" --protected-resource
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Usa il AWS CLI comando seguente per abilitare Malware Protection for S3 per un bucket con prefissi di oggetti specifici e senza tag per gli oggetti S3 scansionati:

```
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"]}}'
```

- Utilizza il seguente AWS CLI comando per abilitare Malware Protection for S3 per un bucket con la codifica degli oggetti S3 scansionati abilitata:

```
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"}
```

Dopo aver eseguito correttamente questi comandi, verrà generato un ID del piano Malware Protection univoco. Per eseguire azioni come l'aggiornamento o la disabilitazione del piano di protezione per il tuo bucket, avrai bisogno di questo ID del piano di protezione da malware.

Per problemi con le autorizzazioni dei ruoli IAM, consulta. [Risoluzione dell'errore relativo alle autorizzazioni dei ruoli IAM](#)

Creare o aggiornare la politica dei ruoli IAM

Per consentire a Malware Protection for S3 di scansionare e (facoltativamente) aggiungere tag agli oggetti S3, puoi utilizzare ruoli di servizio che dispongono delle autorizzazioni necessarie per eseguire azioni di scansione del malware per tuo conto. [Per ulteriori informazioni sull'utilizzo dei ruoli di servizio per abilitare la protezione da malware per S3, consulta Service Access.](#) Questo ruolo è diverso dal ruolo collegato al [servizio GuardDuty Malware Protection](#).

Se preferisci utilizzare i ruoli IAM, puoi associare un ruolo IAM che include le autorizzazioni necessarie per eseguire la scansione e (facoltativamente) aggiungere tag agli oggetti S3. È necessario creare un ruolo IAM o aggiornare un ruolo esistente per includere queste autorizzazioni. Poiché queste autorizzazioni sono necessarie per ogni bucket Amazon S3 per il quale abiliti Malware Protection for S3, devi eseguire questo passaggio per ogni bucket Amazon S3 da proteggere.

L'elenco seguente spiega in che modo determinate autorizzazioni aiutano a GuardDuty eseguire la scansione antimalware per tuo conto:

- Consenti ad Amazon EventBridge Actions di creare e gestire la regola EventBridge gestita in modo che Malware Protection for S3 possa ascoltare le notifiche degli oggetti S3.

Per ulteriori informazioni, consulta [Amazon EventBridge managed rules](#) nella Amazon EventBridge User Guide.

- Consenti ad Amazon S3 e alle EventBridge azioni di inviare notifiche per tutti gli eventi in questo bucket EventBridge

Per ulteriori informazioni, consulta [Enabling Amazon EventBridge](#) nella Amazon S3 User Guide.

- Consenti alle azioni di Amazon S3 di accedere all'oggetto S3 caricato e aggiungi un tag predefinito all'oggetto S3 GuardDutyMalwareScanStatus scansionato. Quando usi un prefisso di oggetto, aggiungi una `s3:prefix` condizione solo sui prefissi di destinazione. Ciò GuardDuty impedisce l'accesso a tutti gli oggetti S3 nel bucket.
- Consenti alle azioni chiave KMS di accedere all'oggetto prima di scansionare e inserire un oggetto di test sui bucket con la crittografia DSSE-KMS e SSE-KMS supportata.

Note

Questo passaggio è necessario ogni volta che attivi Malware Protection for S3 per un bucket nel tuo account. Se disponi già di un ruolo IAM, puoi aggiornarne la policy per includere i

dettagli di un'altra risorsa bucket Amazon S3. L'[Aggiungere le autorizzazioni delle policy IAM](#) argomento fornisce un esempio su come eseguire questa operazione.

Utilizza le seguenti politiche per creare o aggiornare un ruolo IAM.

Policy

- [Aggiungere le autorizzazioni delle policy IAM](#)
- [Aggiungere una politica di relazione di fiducia](#)

Aggiungere le autorizzazioni delle policy IAM

Puoi scegliere di aggiornare la policy in linea di un ruolo IAM esistente o creare un nuovo ruolo IAM. Per informazioni sui passaggi, consulta [Creazione di un ruolo IAM](#) o [Modifica della politica di autorizzazione di un ruolo](#) nella Guida per l'utente IAM.

Aggiungi il seguente modello di autorizzazioni al tuo ruolo IAM preferito. Sostituisci i seguenti valori segnaposto con i valori appropriati associati al tuo account:

- Infatti *amzn-s3-demo-bucket*, sostituiscilo con il nome del tuo bucket Amazon S3.

Per utilizzare lo stesso ruolo IAM per più di una risorsa bucket S3, aggiorna una policy esistente come mostrato nell'esempio seguente:

```
...  
...  
"Resource": [  
    "arn:aws:s3:::amzn-s3-demo-bucket/*",  
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"  
],  
...  
...
```

Assicurati di aggiungere una virgola (,) prima di aggiungere un nuovo ARN associato al bucket S3. Esegui questa operazione ogni volta che fai riferimento a un bucket Resource S3 nel modello di policy.

- Perché *111122223333*, sostituiscilo con il tuo Account AWS ID.
- Perché *us-east-1*, sostituisci con il tuo Regione AWS.

- Perché **APKAEIBAERJR2EXAMPLE**, sostituiscilo con il tuo ID chiave gestito dal cliente. Se il tuo bucket S3 è crittografato utilizzando una AWS KMS chiave, aggiungiamo le autorizzazioni pertinenti se scegli l'opzione [Crea un nuovo ruolo](#) durante la configurazione della protezione da malware per il tuo bucket.

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

Modello di policy sui ruoli 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/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ],
    "Condition": {
      "StringLike": {
        "events:ManagedBy": "malware-protection-plan.guarddduty.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
    "Effect": "Allow",
    "Action": [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource": [
```

```

        "arn:aws:events:us-east-1:111122223333:rule/D0-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"
        }
    }
}
]
}

```

Aggiungere una politica di relazione di fiducia

Allega la seguente politica di fiducia al tuo ruolo IAM. Per informazioni sui passaggi, consulta [Modifica di una policy di fiducia per i ruoli](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Risoluzione dell'errore relativo alle autorizzazioni dei ruoli IAM

Quando abiliti Malware Protection for S3, GuardDuty verifica se il tuo ruolo di servizio IAM dispone delle autorizzazioni necessarie per convalidare la proprietà del bucket Amazon S3. Se queste autorizzazioni sono mancanti o non sono configurate correttamente, potresti ricevere il seguente messaggio:

```
"message": "The request was rejected because provided IAM role does not have the
  required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Gli scenari seguenti possono aiutarti a risolvere questo errore:

Autorizzazioni per i ruoli IAM mancanti

- Il ruolo IAM deve disporre delle autorizzazioni necessarie per consentire a Malware Protection for S3 di assumere il ruolo.
- GuardDuty convalida la proprietà del bucket con l'autorizzazione. "s3:ListBucket" Questo deve essere presente nel ruolo IAM che utilizzi.

Per informazioni sulle autorizzazioni, consulta [Creare o aggiornare la politica dei ruoli IAM](#).

Disponibilità dei ruoli IAM

- Quando crei un nuovo ruolo IAM, attendi alcuni minuti affinché le modifiche raggiungano la coerenza finale prima di abilitare Malware Protection for S3. Se tenti di abilitare il piano di protezione subito dopo aver creato il ruolo, la convalida potrebbe fallire.
- Per le implementazioni Infrastructure as Code (IaC), GuardDuty consiglia di dichiarare una dipendenza dalle risorse per garantire che il ruolo IAM raggiunga la coerenza finale.

[Per modelli di esempio su come eseguire questa operazione, consulta il repository. GuardDuty GitHub](#)

Abilitazione tra regioni

Assicurati che il tuo bucket Amazon S3 si trovi nella stessa regione in cui stai abilitando Malware Protection for S3. GuardDuty

Passaggi dopo l'attivazione di Malware Protection for S3

Questa sezione elenca i passaggi che è possibile eseguire dopo aver abilitato Malware Protection for S3 per un bucket. I seguenti passaggi sono elencati in un ordine che ti aiuterà a navigare nei passaggi successivi:

Da seguire dopo aver abilitato Malware Protection for S3 per il tuo bucket

1. Aggiungi una politica delle risorse per il controllo degli accessi basata su tag (TBAC): quando abiliti il tagging, prima che un oggetto venga caricato nel bucket selezionato, assicurati di aggiungere la policy TBAC alla risorsa del bucket S3. Per ulteriori informazioni, consulta [Aggiungere TBAC alla risorsa bucket S3](#).
2. Monitora lo stato del piano di protezione da malware: monitora la colonna Status per ogni bucket protetto. Per informazioni sui potenziali stati e sul loro significato, consulta. [Visualizzazione e comprensione dello stato del bucket protetto](#)
3. Avvia una scansione scegliendo una delle seguenti opzioni:
 - Carica un oggetto:
 1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
 2. Carica un file nel bucket S3 o nel prefisso dell'oggetto per cui hai abilitato questa funzionalità. Per la procedura di caricamento di un file, consulta [Caricare un oggetto nel bucket](#) nella Amazon S3 User Guide.

- Avvia una scansione su richiesta: [Scansione malware su richiesta per S3 GuardDuty](#)
4. Monitora lo stato e i risultati della scansione degli oggetti S3: questo passaggio include informazioni su come controllare lo stato della scansione antimalware dell'oggetto S3.

Sono abilitati entrambi GuardDuty e Malware Protection for S3	Protezione da malware abilitata solo per S3
• Quando GuardDuty è abilitata, può generare un messaggio Protezione da malware per tipo di ricerca S3 che indica la presenza di malware nell'oggetto S3 scansionato. • Puoi potenzialmente controllare il risultato della scansione degli oggetti S3 utilizzando una o più opzioni sotto. Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3 Questi includono l'utilizzo di Amazon EventBridge, le CloudWatch metriche per il piano Malware Protection e l'etichettatura degli oggetti scansionati.	È possibile verificare il risultato della scansione degli oggetti S3 utilizzando una o più opzioni riportate di seguito. Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3 Questi includono l'utilizzo di Amazon EventBridge, le CloudWatch metriche per il piano Malware Protection e l'etichettatura degli oggetti scansionati.

Scansione malware su richiesta per S3 GuardDuty

GuardDuty Malware Protection for S3 monitora continuamente i nuovi caricamenti su S3. Per gli oggetti che esistevano prima dell'attivazione della protezione o per eseguire nuovamente la scansione di oggetti scansionati in precedenza, puoi avviare una scansione antimalware S3 su richiesta dopo aver abilitato il piano Malware Protection per il tuo bucket. GuardDuty

La scansione antimalware su richiesta utilizza il ruolo IAM di Malware Protection Plan per l'accesso agli oggetti e l'applicazione della configurazione. La scansione sovrascriverà qualsiasi prefisso configurato nel Malware Protection Plan per il bucket.

Note

La quota Malware Protection for S3 si applica alla scansione antimalware su richiesta. Per ulteriori informazioni, vedere. [Quote nella protezione da malware per S3](#)

Per ulteriori informazioni sui prezzi, consultare [Prezzi e costi di utilizzo di Malware Protection for S3](#).

Prerequisiti

Prima di avviare una scansione antimalware su richiesta, l'account deve soddisfare i seguenti prerequisiti:

- La protezione da malware per S3 è abilitata nel bucket di destinazione. Per ulteriori informazioni, consulta [Configurazione della protezione da malware per S3 per il tuo bucket](#).
- La [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#) policy è allegata all'utente IAM o al ruolo IAM che richiama l'API.

Avvia una scansione antimalware su richiesta

Utilizza l'operazione [SendObjectMalwareScan](#) API, che richiede il percorso dell'oggetto S3 come input.

API/CLI

È possibile scansionare la versione più recente dell'oggetto o specificare una versione particolare da scansionare.

Per scansionare una versione specifica di un oggetto:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket":  
  "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE", "VersionId":  
  "d41d8cd98f00b204e9800998eEXAMPLE"}'
```

Per scansionare la versione più recente di un oggetto:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket": "amzn-s3-demo-  
bucket", "Key": "APKAEIBAERJR2EXAMPLE"}'
```

⚠ Important

Una chiamata API riuscita conferma che la richiesta di scansione è stata accettata. Tuttavia, è importante monitorare i risultati della scansione per garantire il completamento corretto e identificare eventuali problemi, come gli errori di accesso all'oggetto. Per ulteriori informazioni, consulta [Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3](#).

Utilizzo del controllo degli accessi basato su tag (TBAC) con Malware Protection for S3

Quando attivi Malware Protection for S3 per il tuo bucket, puoi facoltativamente scegliere di abilitare i tag. Dopo aver tentato di scansionare un oggetto S3 appena caricato nel bucket selezionato, GuardDuty aggiunge un tag all'oggetto scansionato per indicare lo stato della scansione del malware. Quando si abilita il tagging, viene associato un costo di utilizzo diretto. Per ulteriori informazioni, consulta [Prezzi e costi di utilizzo di Malware Protection for S3](#).

GuardDuty utilizza un tag predefinito con la chiave `as GuardDutyMalwareScanStatus` e il valore come uno degli stati di scansione del malware. Per informazioni su questi valori, vedere [the section called "Potenziale stato di scansione dell'oggetto S3 e stato dei risultati"](#)

Considerazioni sull'aggiunta GuardDuty di un tag all'oggetto S3:

- Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto. Per ulteriori informazioni, consulta [Categorizzazione dello storage mediante tag nella Guida](#) per l'utente di Amazon S3.

Se tutti e 10 i tag sono già in uso, non è GuardDuty possibile aggiungere il tag predefinito all'oggetto scansionato. GuardDuty pubblica inoltre il risultato della scansione nel bus degli eventi predefinito EventBridge . Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#).

- Se il ruolo IAM selezionato non include l'autorizzazione GuardDuty per taggare l'oggetto S3, anche con l'etichettatura abilitata per il bucket protetto, non GuardDuty sarà possibile aggiungere tag a questo oggetto S3 scansionato. Per ulteriori informazioni sull'autorizzazione del ruolo IAM richiesta per l'etichettatura, consulta [Creare o aggiornare la politica dei ruoli IAM](#)

GuardDuty pubblica inoltre il risultato della scansione nel bus EventBridge degli eventi predefinito. Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#).

Aggiungere TBAC alla risorsa bucket S3

Puoi utilizzare le policy delle risorse del bucket S3 per gestire il controllo degli accessi basato su tag (TBAC) per i tuoi oggetti S3. Puoi fornire l'accesso a utenti specifici per accedere e leggere l'oggetto S3. Se hai un'organizzazione creata utilizzando AWS Organizations, devi fare in modo che nessuno possa modificare i tag aggiunti da GuardDuty. Per ulteriori informazioni, consulta [Impedire che i tag vengano modificati se non da soggetti autorizzati nella Guida](#) per l'AWS Organizations utente. L'esempio utilizzato nell'argomento collegato cita `ec2`. Quando utilizzate questo esempio, sostituitelo `ec2` con `s3`.

L'elenco seguente spiega cosa è possibile fare utilizzando TBAC:

- Impedisce a tutti gli utenti tranne il responsabile del servizio Malware Protection for S3 di leggere gli oggetti S3 che non sono ancora etichettati con la seguente coppia chiave-valore di tag:

GuardDutyMalwareScanStatus:*Potential key value*

- Consenti solo GuardDuty di aggiungere la chiave del tag GuardDutyMalwareScanStatus con valore come risultato della scansione a un oggetto S3 scansionato. Il seguente modello di policy può consentire a utenti specifici che dispongono dell'accesso di sovrascrivere potenzialmente la coppia chiave-valore del tag.

Esempio di policy sulle risorse del bucket S3:

Sostituisci i seguenti valori segnaposto nella politica di esempio:

- *IAM-role-name*- Fornisci nel tuo bucket il ruolo IAM che hai usato per configurare Malware Protection for S3.
- *555555555555*- Fornisci il bucket Account AWS associato al bucket protetto.
- *amzn-s3-demo-bucket*- Fornisci il nome del bucket protetto.

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"
      }
    }
  }
}
```

```
}  
  ]  
}
```

Per ulteriori informazioni sull'etichettatura delle risorse S3, consulta le politiche di [tagging](#) e controllo degli accessi.

Visualizzazione e comprensione dello stato del bucket protetto

Dopo aver abilitato Malware Protection for S3 per un bucket, lo stato indica se la funzionalità è configurata e funziona come previsto. Questo stato è associato a un identificatore (ID) del piano Malware Protection univoco. GuardDuty crea questo ID al momento dell'attivazione della funzionalità.

Utilizza la seguente procedura per visualizzare lo stato del tuo bucket protetto:

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, seleziona Malware Protection for S3.
3. Nella tabella Bucket protetti, visualizza la colonna Stato corrispondente al tuo bucket S3.

La tabella seguente elenca e descrive i valori di stato associati alla risorsa del piano Malware Protection. Comprendendo cosa significano questi stati per il tuo bucket protetto, puoi assicurarti meglio che GuardDuty avvii una scansione antimalware automatica quando un oggetto viene caricato.

Status	Description
Attivo	Il tuo bucket S3 è stato configurato con successo con Malware Protection for S3. Quando lo stato è Attivo, le modifiche al ruolo IAM (eliminazione o modifica delle autorizzazioni) non aggiornano lo stato a Avviso o Errore. Consigliamo di monitorare continuamente lo stato della scansione utilizzando uno dei metodi descritti in Monitoraggio delle scansioni degli oggetti S3.

Status	Description
Avvertenza [*] -	Malware Protection for S3 è progettato per non essere influenzato dalla visualizzazione di un avviso. Quando GuardDuty rileva un nuovo oggetto S3, avvierà una scansione antimalware. Dopo aver avviato correttamente la scansione, il valore della colonna Status potrebbe impiegare alcuni minuti per passare ad Attivo. Riceverai una EventBridge notifica dopo l'aggiornamento del valore della colonna Status.
Errore [*] -	Il tuo bucket non è protetto. Nessuna delle scansioni antimalware associate a questo bucket S3 verrà completata. Potrebbero esserci una o più cause potenziali.

* Per informazioni sui potenziali problemi e sui passaggi corrispondenti per risolverli, vedere [Risoluzione dei problemi relativi allo stato del piano di protezione contro](#).

Monitoraggio delle scansioni degli oggetti S3 in Malware Protection for S3

Quando si utilizza Malware Protection for S3 con un ID GuardDuty rilevatore, se l'oggetto Amazon S3 è potenzialmente dannoso GuardDuty, viene generato. [Protezione da malware per tipo di ricerca S3](#) Utilizzando la GuardDuty console e APIs, puoi visualizzare i risultati generati. Per informazioni sulla comprensione di questo tipo di risultato, vedere [Dettagli degli esiti](#).

Quando si utilizza Malware Protection for S3 senza attivarlo GuardDuty (nessun ID rilevatore), anche quando l'oggetto Amazon S3 scansionato è potenzialmente dannoso, non è GuardDuty possibile generare alcun risultato.

Indice

- [Potenziale stato di scansione dell'oggetto S3 e stato dei risultati](#)
- [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#)
- [Monitoraggio delle scansioni degli oggetti S3 con tag gestiti GuardDuty](#)
- [Metriche dello stato di scansione degli oggetti S3 in CloudWatch](#)

Potenziale stato di scansione dell'oggetto S3 e stato dei risultati

Questa sezione spiega i potenziali valori dello stato di scansione degli oggetti S3 e i valori dei risultati della scansione.

Lo stato di scansione di un oggetto S3 indica lo stato della scansione antimalware, ad esempio completata, ignorata o non riuscita.

Lo stato del risultato di una scansione antimalware di un oggetto S3 indica il risultato della scansione in base al valore dello stato della scansione. Il valore dello stato del risultato di una scansione antimalware corrisponde a uno stato di scansione.

L'elenco seguente fornisce i potenziali valori dei risultati della scansione degli oggetti S3. Se hai abilitato l'etichettatura, puoi monitorare il risultato della scansione tramite. [Utilizzo dei tag degli oggetti S3](#) Dopo la scansione, il valore del tag avrà uno dei seguenti valori di risultato della scansione.

Il potenziale malware dell'oggetto S3, i valori dello stato dei risultati della scansione

- **NO_THREATS_FOUND**— non è GuardDuty stata rilevata alcuna potenziale minaccia associata all'oggetto scansionato.
- **THREATS_FOUND**— GuardDuty ha rilevato una potenziale minaccia associata all'oggetto scansionato.
- **UNSUPPORTED**— Esistono alcuni motivi per cui Malware Protection for S3 salterà una scansione. Le possibili ragioni includono file protetti da password, archivi con rapporti di compressione estremamente elevati e il supporto per alcune [Protezione da malware per le quote S3](#) funzionalità di Amazon S3 potrebbe non essere disponibile. Per ulteriori informazioni, consulta [Funzionalità di protezione da malware per S3](#).
- **ACCESS_DENIED**— non GuardDuty riesco ad accedere a questo oggetto per la scansione. Controlla le autorizzazioni del ruolo IAM associate a questo bucket. Per ulteriori informazioni, consulta [Creare o aggiornare la politica dei ruoli IAM](#).

Se hai abilitato il tagging degli oggetti S3 dopo la scansione, vedi. [Risoluzione dei problemi relativi agli errori dei tag post-scansione degli oggetti S3](#)

- **FAILED**— impossibile GuardDuty eseguire la scansione antimalware su questo oggetto a causa di un errore interno.

L'elenco seguente fornisce i potenziali valori dello stato di scansione degli oggetti S3 e la loro mappatura al risultato della scansione degli oggetti S3.

Valori potenziali dello stato di scansione degli oggetti S3

- **Completata:** la scansione è stata completata correttamente e indica se l'oggetto S3 contiene malware. In questo caso, il potenziale valore del risultato della scansione degli oggetti S3 potrebbe essere uno dei due `THREATS_FOUND` o `NO_THREATS_FOUND`.
- **Ignorato:** GuardDuty salta una scansione antimalware quando la scansione di questo oggetto S3 non è supportata da Malware Protection for S3 o GuardDuty non ha accesso all'oggetto S3 caricato nel bucket selezionato.

In questo caso, il potenziale valore del risultato della scansione degli oggetti S3 potrebbe essere o. `UNSUPPORTED_ACCESS_DENIED`

GuardDuty salterà inoltre la scansione se il ruolo IAM richiesto viene eliminato.

- **Fallito:** analogamente al valore del risultato della scansione degli oggetti S3 `FAILED`, questo stato di scansione indica che non GuardDuty è stato possibile eseguire la scansione antimalware sull'oggetto S3 a causa di un errore interno.

Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge

Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, applicazioni Software-as-a-Service (SaaS) e AWS servizi e indirizza tali dati verso destinazioni come Lambda. In questo modo puoi monitorare gli eventi che si verificano nei servizi e creare architetture basate su eventi. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

In qualità di account proprietario di un bucket S3 protetto con Malware Protection for S3, GuardDuty pubblica EventBridge notifiche sul bus degli eventi predefinito nei seguenti scenari:

- Modifiche allo stato delle risorse del piano Malware Protection per tutti i bucket protetti. Per informazioni sui vari stati, vedere. [Visualizzazione e comprensione dello stato del bucket protetto](#)

Per configurare la regola Amazon EventBridge (EventBridge) per lo stato delle risorse, consulta [Stato delle risorse del piano Malware Protection](#).

- Il risultato della scansione degli oggetti S3 viene pubblicato sul bus degli EventBridge eventi predefinito.

Il `s3Throttled` campo indica se si è verificato un ritardo nel caricamento o nel recupero dello storage da Amazon S3. Il valore `true` indica che c'è stato un ritardo e `false` indica che non c'è stato alcun ritardo.

Se `s3Throttled` si tratta `true` del risultato della scansione, Amazon S3 consiglia di impostare i prefissi in modo da ridurre le transazioni al secondo (TPS) per ogni prefisso. Per ulteriori informazioni, consulta [Modelli di progettazione basati sulle best practice: ottimizzazione delle prestazioni di Amazon S3](#) nella Amazon S3 User Guide.

Per configurare la regola Amazon EventBridge (EventBridge) per i risultati della scansione degli oggetti S3, consulta [Risultato della scansione degli oggetti S3](#).

- Si verifica un errore del tag post-scan per i seguenti motivi:
 - Al tuo ruolo IAM mancano le autorizzazioni per etichettare l'oggetto.

Il [Aggiungere le autorizzazioni delle policy IAM](#) modello include l'autorizzazione per GuardDuty etichettare un oggetto.

- La risorsa o l'oggetto del bucket specificato nel ruolo IAM non esiste più.
- L'oggetto S3 associato ha già raggiunto il limite massimo di tag. Per ulteriori informazioni sul limite di tag, consulta [Categorizzazione dello storage mediante tag nella Guida](#) per l'utente di Amazon S3.

Per configurare la regola Amazon EventBridge (EventBridge) per gli eventi di errore dei tag post-scan, consulta [Eventi di errore del tag post-scansione](#).

Imposta le regole EventBridge

Puoi impostare EventBridge delle regole nel tuo account per inviare lo stato delle risorse, gli eventi di errore dei tag post-scansione o il risultato della scansione degli oggetti S3 a un altro. Servizio AWS In qualità di account GuardDuty amministratore delegato, riceverai la notifica sullo stato delle risorse del piano Malware Protection in caso di modifica dello stato.

Verranno applicate le EventBridge tariffe standard. Per ulteriori informazioni, consulta i [EventBridge prezzi di Amazon](#).

Tutti i valori visualizzati in **red** sono segnaposto per l'esempio. Questi valori cambieranno in base ai valori del tuo account e al fatto che venga rilevato o meno malware.

Argomenti

- [Stato delle risorse del piano Malware Protection](#)
- [Risultato della scansione degli oggetti S3](#)
- [Eventi di errore del tag post-scansione](#)

Stato delle risorse del piano Malware Protection

È possibile creare un modello di EventBridge evento basato sui seguenti scenari:

detail-type Valori potenziali

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"
- "GuardDuty Malware Protection Resource Status Error"

Modello di evento

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guardduty"]
}
```

Schema di notifica di esempio per **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"
  }
}

```

Schema di notifica di esempio per **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"
      }
    ]
  }
}

```

Schema di notifica di esempio per **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"
        }
      ]
    }
  }
}

```

In base al motivo alla base di resourceStatusERROR, il statusReasons valore verrà compilato.

Per informazioni sulla procedura di risoluzione dei problemi relativi ai seguenti avvisi ed errori, vedere [Risoluzione dei problemi relativi allo stato del piano di protezione contro](#).

Risultato della scansione degli oggetti S3

```

{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}

```

Schema di notifica di esempio per **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
  }
}
}

```

Schema di notifica di esempio per **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)"
            }
        ]
    }
}

```

Note

Il `scanResultDetails.Threats` campo contiene solo una minaccia. Per impostazione predefinita, la scansione Malware Protection for S3 riporta la prima minaccia rilevata. Dopodiché, `scanStatus` è impostato su `COMPLETED`.

Schema di notifica di esempio per lo stato dei risultati della scansione **UNSUPPORTED** (Ignorato):

```

{
  "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
    }
  }
}

```



```

    }
  }
}

```

Schema di notifica di esempio per lo stato dei risultati della scansione **ACCESS_DENIED** (Ignorato):

```

{
  "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
    }
  }
}

```

Schema di notifica di esempio per lo stato **FAILED** dei risultati della scansione:

```

{
  "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
      }
    }
  }
}

```

Eventi di errore del tag post-scansione

Schema dell'evento:

```

{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty"
}

```

Schema di notifica di esempio per **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"
    }]
  }
}

```

Schema di notifica di esempio per **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"
    }]
  }
}

```

```
}
```

Per risolvere questi motivi di errore, vedere. [Risoluzione dei problemi relativi agli errori dei tag post-scansione degli oggetti S3](#)

Monitoraggio delle scansioni degli oggetti S3 con tag gestiti GuardDuty

Utilizza l'opzione di abilitazione dei tag in modo da GuardDuty poter aggiungere tag al tuo oggetto Amazon S3 dopo aver completato la scansione del malware.

Considerazioni sull'abilitazione dei tag

- È previsto un costo di utilizzo associato all'etichettatura degli GuardDuty oggetti S3. Per ulteriori informazioni, consulta [Prezzi e costi di utilizzo di Malware Protection for S3](#).
- È necessario mantenere le autorizzazioni di etichettatura richieste per il ruolo IAM preferito associato a questo bucket; in caso contrario, non è GuardDuty possibile aggiungere tag agli oggetti scansionati. Il ruolo IAM include già le autorizzazioni per aggiungere tag agli oggetti S3 scansionati. Per ulteriori informazioni, consulta [Creare o aggiornare la politica dei ruoli IAM](#).
- Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto S3. Per ulteriori informazioni, consulta [Utilizzo del controllo degli accessi basato su tag \(TBAC\)](#).

Dopo aver abilitato il tagging per un bucket S3 o per prefissi specifici, a ogni oggetto appena caricato che viene scansionato verrà associato un tag nel seguente formato di coppia chiave-valore:

GuardDutyMalwareScanStatus:*Scan-Result-Status*

Per informazioni sui potenziali valori dei tag, consulta. [Potenziale stato di scansione dell'oggetto S3 e stato dei risultati](#)

Risoluzione degli errori dei tag post-scansione degli oggetti S3 in Malware Protection for S3

Questa sezione si applica solo agli utenti che utilizzano il [Abilita l'etichettatura per gli oggetti scansionati](#) bucket protetto.

Quando si GuardDuty tenta di aggiungere un tag all'oggetto S3 scansionato, l'azione di tagging può avere esito negativo. I potenziali motivi per cui ciò può accadere al tuo bucket sono e. ACCESS_DENIED MAX_TAG_LIMIT_EXCEEDED Utilizza i seguenti argomenti per comprendere i potenziali motivi di questi motivi di errore dei tag post-scansione e risolverli.

ACCESS_DENIED

L'elenco seguente fornisce i potenziali motivi che possono causare questo problema:

- Il ruolo IAM utilizzato per questo bucket S3 protetto non dispone dell'AllowPostScanTagautorizzazione. Verifica che il ruolo IAM associato utilizzi questa policy del bucket. Per ulteriori informazioni, consulta [Creare o aggiornare la politica dei ruoli IAM](#).
- La policy protetta del bucket S3 non consente di aggiungere tag GuardDuty a questo oggetto.
- L'oggetto S3 scansionato non esiste più.

MAX_TAG_LIMIT_EXCEEDED

Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto S3. Per ulteriori informazioni, consulta Considerazioni sull'aggiunta GuardDuty di un tag all'oggetto S3 nella sezione. [Abilita l'etichettatura per gli oggetti scansionati](#)

Metriche dello stato di scansione degli oggetti S3 in CloudWatch

È possibile monitorare GuardDuty l'utilizzo CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per 15 mesi, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni di Malware Protection for S3. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

Le CloudWatch metriche per Malware Protection for S3 sono disponibili a livello di risorsa. Puoi interrogare queste metriche per ogni risorsa protetta separatamente. Le metriche sono riportate nel namespace. AWS/GuardDuty/MalwareProtection È possibile impostare allarmi su risorse specifiche per monitorare il livello di sicurezza.

Metriche dello stato della scansione antimalware

Parametro	Descrizione
CompletedScanCount	Il numero di scansioni antimalware di oggetti S3 completate in un determinato periodo di tempo.
	Dimensioni valide:
	• Malware Protection Plan Id

Resource Name

Unità: numero

FailedScanCount

Il numero di scansioni di malware relative agli oggetti S3 non riuscite in un determinato periodo di tempo.

Dimensioni valide:

- Malware Protection Plan Id

Resource Name

Unità: numero

SkippedScanCount

Il numero di scansioni di malware a oggetti S3 che sono state ignorate in un determinato periodo di tempo.

Dimensioni valide:

- Malware Protection Plan Id

Resource Name

Skipped Reason

Valori potenziali

- Unsupported
- MissingPermissions

Unità: numero

Metriche dei risultati della scansione del malware

InfectedScanCount

Il numero di scansioni di malware su oggetti S3 che hanno rilevato oggetti potenzialmente dannosi in un determinato periodo di tempo.

Dimensioni valide:

- Malware Protection Plan Id

Resource Name

Unità: numero

CompletedScanBytes

Il numero di byte di oggetti S3 scansionati in un determinato periodo di tempo.

Dimensioni valide:

- Malware Protection Plan Id

Resource Name

Unità: numero

 Note

Per impostazione predefinita, le statistiche nelle CloudWatch metriche sono AVG.

Le seguenti dimensioni sono supportate per le metriche Malware Protection for S3.

Dimensione**Descrizione**

Malware Protection Plan Id

L'identificatore univoco associato alla risorsa del piano Malware Protection GuardDuty creata per la risorsa protetta.

Resource Name

Il nome della risorsa protetta.

Skipped Reason

Il motivo per cui una scansione antimalware di oggetti S3 è stata ignorata.

Valori potenziali

- Unsupported
- MissingPermissions

Per informazioni sull'accesso e sull'interrogazione di questi parametri, consulta Use [Amazon CloudWatch metrics nella Amazon CloudWatch](#) User Guide.

Per informazioni sulla configurazione degli allarmi, consulta [Using Amazon CloudWatch alarms](#) nella Amazon CloudWatch User Guide.

Risoluzione dei problemi

Indice

- [Risoluzione dei problemi relativi allo stato del piano di protezione contro](#)
- [Risoluzione dei problemi relativi alla scansione antimalware su richiesta](#)

Risoluzione dei problemi relativi allo stato del piano di protezione contro

Per ogni bucket protetto, GuardDuty visualizza lo stato in base alla classifica. Ad esempio, se un bucket protetto presenta problemi nelle categorie Errore e Avviso, GuardDuty visualizza innanzitutto il problema associato allo stato di errore.

L'elenco seguente include gli errori e gli avvisi relativi allo stato del piano Malware Protection.

Errori

- [EventBridge la notifica è disabilitata per questo bucket S3](#)
- [EventBridge manca una regola gestita per ricevere gli eventi del bucket S3](#)
- [Il bucket S3 non esiste più](#)

Attenzione

[Impossibile inserire l'oggetto di prova](#)

EventBridge la notifica è disabilitata per questo bucket S3

Il codice del motivo dello stato associato è.

EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED

Dettagli sullo stato

GuardDuty utilizza EventBridge per ricevere una notifica quando un nuovo oggetto viene caricato in questo bucket S3. Questa autorizzazione non è presente nel tuo ruolo IAM.

Passaggi per la risoluzione dei problemi

Opzione 1: aggiungi la seguente dichiarazione di autorizzazione al tuo ruolo IAM:

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
}
```

amzn-s3-demo-bucket Sostituiscilo con il nome del tuo bucket Amazon S3.

Opzione 2: abilitare le EventBridge notifiche utilizzando la console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella pagina Bucket, nella scheda General purpose buckets, seleziona il nome del bucket associato a questo errore.
3. In questa pagina del bucket, scegli la scheda Proprietà.
4. Nella EventBridge sezione Amazon, seleziona Modifica.
5. Nella EventBridge pagina Modifica Amazon, per Invia notifica ad Amazon EventBridge per tutti gli eventi in questo bucket, seleziona Attiva.
6. Scegli Save changes (Salva modifiche).

Potrebbero essere necessari alcuni minuti prima che il valore della colonna Status diventi Attivo.

EventBridge manca una regola gestita per ricevere gli eventi del bucket S3

Il codice del motivo dello stato associato è. EVENTBRIDGE_MANAGED_RULE_DISABLED

Dettagli sullo stato

Mancano le autorizzazioni EventBridge gestite per gestire la configurazione delle EventBridge regole.

Passaggi per la risoluzione dei problemi

Aggiungi la seguente dichiarazione di autorizzazione al tuo ruolo 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"
    }
  }
}
```

Potrebbero essere necessari alcuni minuti prima che il valore della colonna Status diventi Attivo.

Il bucket S3 non esiste più

Il codice del motivo dello stato associato è. PROTECTED_RESOURCE_DELETED

Dettagli sullo stato

Questo bucket S3 è stato eliminato dal tuo account e non esiste più.

Passaggio 2 per la risoluzione dei problemi

Se l'eliminazione del bucket S3 non è stata intenzionale, puoi creare un nuovo bucket utilizzando la console Amazon S3.

Dopo aver creato il bucket con successo, abilita Malware Protection for S3 seguendo i passaggi indicati nella pagina. [Configurazione della protezione da malware per S3 per il tuo bucket](#)

Impossibile inserire l'oggetto di prova

Il codice del motivo dello stato associato è `INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

Note

L'autorizzazione ad aggiungere un oggetto di test è facoltativa. La mancanza di questa autorizzazione nel tuo ruolo IAM non impedisce a Malware Protection for S3 di avviare una scansione antimalware su un oggetto appena caricato. Una volta avviata correttamente una scansione, potrebbero essere necessari alcuni minuti prima che lo stato del piano di protezione contro il malware passi da Avviso ad Attivo.

Se il ruolo IAM include già questa autorizzazione, questo avviso indica una policy restrittiva per i bucket Amazon S3 che non consente all'accesso IAM di inserire l'oggetto di test in questo bucket S3.

Dettagli sullo stato

Per convalidare la configurazione del bucket selezionato, GuardDuty inserisce un oggetto di test nel bucket.

Passaggi per la risoluzione dei problemi

Puoi scegliere di aggiornare il ruolo IAM per includere le autorizzazioni mancanti. Al ruolo IAM selezionato, aggiungi le seguenti autorizzazioni in modo da GuardDuty poter inserire l'oggetto di test nella risorsa selezionata:

```
{
    "Sid": "AllowPutValidationObject",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
```

```
    ],  
    "Resource": [  
        "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-  
object"  
    ]  
}
```

amzn-s3-demo-bucket Sostituiscilo con il nome del tuo bucket Amazon S3. Per informazioni sulle autorizzazioni dei ruoli IAM, consulta. [Creare o aggiornare la politica dei ruoli IAM](#)

Potrebbero essere necessari alcuni minuti prima che il valore della colonna Status diventi Attivo.

Risoluzione dei problemi relativi alla scansione antimalware su richiesta

Impossibile avviare una scansione.

Assicurati che la richiesta di scansione contenga un input valido e che il Malware Protection Plan sia abilitato per il bucket.

Modifica del piano di protezione da malware per un bucket protetto

Potrebbe essere necessario modificare la politica di autorizzazione IAM preferita, abilitare o disabilitare il tagging dell'oggetto S3 scansionato o aggiungere o rimuovere i prefissi degli oggetti S3. Ad esempio, quando hai abilitato Malware Protection for S3 per il tuo bucket, hai deciso di non abilitare l'etichettatura dell'oggetto S3 scansionato con il risultato della scansione. Tuttavia, ora desideri GuardDuty aggiungere il tag predefinito e il risultato della scansione come valore del tag.

Scegli un metodo di accesso preferito per aggiornare il piano di protezione da malware per il tuo bucket S3 protetto.

Console

Per modificare un piano di protezione da malware

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione, scegli Malware Protection for S3.
3. In Bucket protetti, seleziona il bucket per il quale desideri modificare la configurazione esistente.

4. Scegli Modifica.
5. Aggiorna la configurazione e le impostazioni esistenti per il tuo bucket e conferma le modifiche. Per informazioni sulla descrizione e sui passaggi per ogni sezione, consulta [Attivazione della protezione da malware per S3 per il tuo bucket](#).

Monitora la colonna Status per questo bucket protetto. Se appare come Avviso o Errore, vedi [Risoluzione dei problemi relativi allo stato del piano di protezione contro](#).

API/CLI

Per modificare il piano di protezione da malware utilizzando l'API o AWS CLI

- Utilizzando l'API

Esegui l'[UpdateMalwareProtectionPlan](#) API utilizzando l'ID del piano Malware Protection associato a questa risorsa del piano.

Per recuperare l'ID del piano Malware Protection in una regione specifica, puoi eseguire l'[ListMalwareProtectionPlans](#) API in quella regione.

- Utilizzando AWS CLI

L'elenco seguente fornisce comandi di AWS CLI esempio per aggiornare la risorsa del piano Malware Protection. Avrai bisogno dell'ID del piano Malware Protection associato al tuo bucket S3.

AWS CLI comandi di esempio

- Utilizza il seguente AWS CLI comando per abilitare o disabilitare il tagging per la risorsa del piano Malware Protection associata al tuo bucket S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
```

- Usa il AWS CLI comando seguente per aggiungere un prefisso di oggetto alla risorsa del piano Malware Protection associata al tuo bucket S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
```

Assicurati di includere i prefissi degli oggetti esistenti in questo comando; in caso contrario, GuardDuty rimuoverà tali prefissi durante la modifica della risorsa del piano Malware Protection.

- Utilizza il AWS CLI comando seguente per rimuovere il prefisso di un oggetto dalla risorsa del piano Malware Protection associata al tuo bucket S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
```

Se non disponi già dell'ID del piano di protezione da malware per questa risorsa, puoi eseguire il AWS CLI comando seguente e sostituirlo **us-east-1** con la regione per la quale desideri elencare il piano di protezione da malware. IDs

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Disattivazione di Malware Protection for S3 per un bucket protetto

Quando disabiliti Malware Protection for S3 per un bucket protetto, GuardDuty elimina l'ID del piano Malware Protection associato a quel bucket. GuardDuty non avvierà più una scansione antimalware quando un nuovo oggetto viene caricato in questo bucket o in uno dei prefissi dell'oggetto selezionati.

Se lo hai abilitato GuardDuty e ora desideri sospenderlo o disabilitarlo, consulta. GuardDuty [Sospensione o disabilitazione GuardDuty](#) Poiché in Malware Protection for S3 non esiste il concetto di ID di rilevamento, la disabilitazione o la sospensione GuardDuty non influiscono sullo stato di un bucket protetto nel tuo account. Puoi continuare a utilizzare la funzionalità Malware Protection for S3 indipendentemente dai prezzi standard associati. Per ulteriori informazioni, consulta [Analisi dei costi di utilizzo di Malware Protection for S3](#). Per smettere di usare Malware Protection for S3, dovrai disabilitarla per tutti i bucket protetti del tuo account. Se desideri continuare a utilizzare GuardDuty e disabilitare solo Malware Protection for S3 per un bucket, i passaggi seguenti non influiranno sulla configurazione del GuardDuty servizio e sugli altri piani di protezione che potresti aver abilitato.

Scegli un metodo di accesso preferito per disabilitare Malware Protection for S3 nel tuo bucket S3 protetto.

Console

Per disabilitare Malware Protection for S3 utilizzando la console GuardDuty

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione, scegli Malware Protection for S3.
3. In Bucket protetti, seleziona il bucket per il quale desideri disabilitare Malware Protection for S3.

Puoi selezionare solo un bucket protetto alla volta. Per disabilitare Malware Protection for S3 per più di un bucket, segui nuovamente questi passaggi per un altro bucket S3.

4. Scegli Disabilita per confermare la selezione.

API/CLI

Per disabilitare Malware Protection for S3 utilizzando l'API o AWS CLI

- Utilizzando l'API

Esegui l'[DeleteMalwareProtectionPlan](#)API utilizzando l'ID del piano Malware Protection associato a questa risorsa del piano.

Per recuperare l'ID del piano Malware Protection, puoi eseguire l'[ListMalwareProtectionPlans](#)API.

- Utilizzando AWS CLI

In alternativa, puoi eseguire il seguente AWS CLI comando per disabilitare Malware Protection for S3 sostituendolo *4cc8bf26c4d75EXAMPLE* con l'ID del piano Malware Protection associato a questo bucket S3:

```
aws guardduty delete-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE
```

Se non disponi già dell'ID del piano di protezione da malware per questo bucket S3, puoi eseguire il AWS CLI comando seguente e sostituirlo *us-east-1* con la regione per la quale desideri elencare il piano di protezione da malware. IDs

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Supportabilità delle funzionalità di Amazon S3

La tabella seguente specifica se Malware Protection for S3 supporta o meno le funzionalità di Amazon S3 elencate.

Il supporto è disponibile?	Description
Sì	Gli oggetti S3 possono essere recuperati senza eseguire il ripristino in modo asincrono.

Il supporto è disponibile?	Description
Condizionale	• Il supporto Intelligent Tiering è disponibile per gli oggetti S3 nei livelli Frequent, Infrequent e Archive Instance Access. • I livelli opt-in Archive e Deep Archive non sono supportati. • Intelligent Tiering crea sempre un nuovo oggetto nel livello Frequent Access. Pertanto, è supportata la scansione degli oggetti durante la creazione. • Le future funzionalità di Intelligent Tiering potrebbero avviare gli oggetti in Archive. Pertanto, questa funzionalità non è supportata.

Il supporto è disponibile?	Description
No	GuardDuty supporta solo bucket generici per Malware Protection for S3.

Il supporto è disponibile?	Description
No	Gli oggetti S3 devono essere ripristinati prima di poter accedervi.
No	La protezione da malware per S3 non è supportata su Outposts.

Il supporto è disponibile?	Description
Sì	Tutti gli oggetti S3 caricati vengono scansionati alla ricerca di malware. Se hai caricato un oggetto con la versione del file v1 e hai immediatamente caricato un'altra versione sostituita con v2, GuardDuty eseguirà la scansione di entrambe le versioni del file oggetto v1 e v2. Tuttavia, l'ora di inizio della scansione potrebbe non essere nello stesso ordine.
Sì	Se il bucket di destinazione è una risorsa protetta, GuardDuty eseguirà la scansione di tutti gli oggetti S3 replicati nei prefissi protetti e monitorati.
No	Non è possibile definire una regola di replica basata sul tag dei risultati della scansione. Amazon S3 non supporta la replica per i tag, ad eccezione di on create.

Il supporto è disponibile?	Description
Sì	GuardDuty supporta scansioni antimalware per oggetti S3 crittografati con chiavi gestite e gestite dal cliente. Assicurati che il ruolo IAM includa l'autorizzazione all'uso della chiave. Per ulteriori informazioni, consulta Aggiungere le autorizzazioni delle policy IAM.

Il supporto è disponibile?	Description
No	Malware Protection for S3 non supporta la scansione di oggetti S3 crittografati con chiavi non accessibili.
No	Quando i tuoi oggetti Amazon S3 vengono crittografati utilizzando Amazon S3 Encryption Client, non vengono esposti a terze parti, inclusi. AWS Per informazioni sul motivo per cui questa funzionalità non è supportata, consulta Protezione dei dati utilizzando la crittografia lato client.  Note Gli oggetti crittografati CSE-KMS vengono ricevuti come blob crittografati in cui non è possibile determinare la crittografia. Pertanto, li GuardDuty elabora non appena vengono ricevuti e analizza il blob crittografato come un normale file. GuardDuty non restituisce uno stato di UNSUPPORTED scansione per tali oggetti, a meno che uno dei due non superi Quote nella protezione da malware per S3.

Il supporto è disponibile?	Description
Sì	Gli oggetti S3 bloccati vengono bloccati in base a WORM - Write Once Read Many. Malware Protection for S3 può accedere e scansionare gli oggetti.
Sì	Malware Protection for S3 può scansionare i bucket configurati con Requester Pays. Il richiedente pagherà le chiamate S3. Per ulteriori informazioni, consulta la sezione Utilizzo dei bucket con pagamento a carico del richiedente per i trasferimenti e l'utilizzo dello storage nella Guida per l'utente di Amazon S3.
Sì	È possibile definire le politiche del ciclo di vita in base al tag dei risultati della scansione. Ad esempio, elimina automaticamente gli oggetti dannosi. Per ulteriori informazioni sulla configurazione del ciclo di vita, consulta Managing your storage lifecycle nella Amazon S3 User Guide.
Sì	Puoi definire le politiche relative alle risorse del bucket in base al tag dei risultati della scansione degli oggetti S3. Ad esempio, impedisce l'accesso agli oggetti S3 che non sono ancora stati scansionati o alle minacce rilevate. GuardDuty Per ulteriori informazioni, consulta Utilizzo del controllo degli accessi basato su tag (TBAC) con Malware Protection for S3 .

Quote nella protezione da malware per S3

Questa sezione fornisce quote predefinite, spesso denominate limiti. Se non diversamente specificato, ogni quota è specifica della regione. Per visualizzare le quote predefinite specifiche per l'utilizzo del servizio di base, vedere GuardDuty [GuardDuty Quote Amazon](#)

Le tabelle seguenti descrivono le quote multiple che verranno applicate alle tue Account AWS

AWS valore di quota predefinito	È regolabile?	Description
100 GB	No	La dimensione massima dell'oggetto S3 che GuardDuty tenterà di eseguire la scansione alla ricerca di malware. Sebbene questa quota non sia regolabile, se hai bisogno di scansionare oggetti più grandi, contatta Supporto AWS per determinare se è GuardDuty possibile aumentare la quota per il tuo caso d'uso.
100 GB	No	La quantità massima di dati che è GuardDuty possibile estrarre e analizzare da un file di archivio. GuardDuty salterà l'estrazione dei file di archivio per una dimensione superiore a 100 GB.
10.000	No	Il numero massimo di file che è GuardDuty possibile estrarre e analizzare in un file di archivio. Se l'archivio contiene più di 10.000 file, GuardDuty sarà necessario saltare il file archiviato.

AWS valore di quota predefinito	È regolabile?	Description
		 Note I tipi di file composti sono potenzialmente soggetti a questi limiti. I tipi di file includono , a titolo esemplificativo, messaggi di posta elettronica codificati MIME (Multipurpose Internet Mail Extensions), file Compiled Python (PYC), file CHM (Compiled HTML Help), tutti i programmi di installazione e documenti Format (ODF). OpenDocument
5	No	I livelli massimi di archivi annidati che è GuardDuty possibile estrarre. Se l'archivio include file nidificati oltre questo valore, GuardDuty ignorerà tali file nidificati.
25	No	Il numero massimo di bucket S3 per i quali è possibile abilitare Malware Protection for S3. Questo limite di quota è per account in ogni regione.

GuardDuty Protezione da malware per il AWS backup

Argomenti

- [Panoramica di](#)
- [Come funziona Malware Protection for Backup?](#)
- [GuardDuty Protezione da malware per il backup: autorizzazioni IAM Role](#)
- [\(Facoltativo\) Inizia a usare Malware Protection for Backup Independently \(solo console\)](#)
- [Avvio di una scansione su richiesta per la protezione da malware per il backup](#)
- [Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for Backup](#)
- [Quote per la protezione da malware per il backup](#)

Panoramica di

Malware Protection for Backup ti aiuta a rilevare la potenziale presenza di malware nei dati di backup mediante la scansione di risorse AWS protette da backup come istantanee di Amazon EBS, Amazon EC2 AMIs e punti di ripristino Amazon S3. Quando AWS Backup crea o aggiorna una risorsa di backup protetta, GuardDuty può eseguire una scansione antimalware su tale backup per identificare contenuti potenzialmente dannosi prima che vengano ripristinati nell'ambiente.

Come utilizzare Malware Protection for Backup

Puoi utilizzare questa funzionalità in due modalità, a seconda che GuardDuty sia abilitata nel tuo account:

1. Utilizzo di Malware Protection for Backup con GuardDuty abilitato

Quando GuardDuty è abilitato in una regione, AWS Backup integra la protezione da malware con il flusso di lavoro dei GuardDuty risultati. I risultati delle scansioni antimalware vengono visualizzati nei GuardDuty risultati oltre che in Amazon EventBridge e Amazon CloudWatch.

2. Utilizzo di Malware Protection for Backup senza abilitare GuardDuty

È possibile utilizzare Malware Protection for Backup in modo indipendente, senza abilitare il GuardDuty servizio completo. In questa modalità, i risultati della scansione rimangono completamente disponibili tramite EventBridge e CloudWatch.

Considerazioni sull'utilizzo indipendente di Malware Protection for Backup

Quando si utilizza la funzionalità senza abilitare GuardDuty:

- La configurazione del piano di backup è gestita interamente in AWS Backup.

GuardDuty non fornisce controlli per la selezione dei piani di backup, degli archivi o dei tipi di risorse. Tutta l'abilitazione, la pianificazione e la configurazione delle policy rimangono in Backup. AWS

- GuardDuty i risultati non vengono generati.

I risultati richiedono un ID del rilevatore, che viene creato solo quando GuardDuty è abilitato. Quando si utilizza Malware Protection in modo indipendente, i risultati della scansione vengono visualizzati esclusivamente attraverso EventBridge eventi e CloudWatch metriche.

- È comunque possibile avviare scansioni su richiesta dalla console. GuardDuty

Anche quando non GuardDuty è abilitata, la GuardDuty console fornisce un flusso di lavoro per avviare una scansione antimalware su richiesta per i tipi di risorse di backup supportati. Ciò consente ai clienti di utilizzare un' GuardDuty interfaccia familiare senza richiedere il GuardDuty servizio completo.

- I non GuardDuty clienti possono accedere ai flussi di lavoro di avvio della scansione.

I punti di accesso alla scansione su richiesta sono disponibili per tutti i clienti che utilizzano Malware Protection for Backup, indipendentemente dal fatto che nell'account sia presente un GuardDuty rilevatore.

- Il comportamento e la copertura della scansione rimangono identici.

Indipendentemente dal fatto che GuardDuty sia abilitata o meno, la funzionalità analizza gli stessi tipi di risorse di AWS Backup con lo stesso motore di rilevamento malware. L'unica differenza è dove vengono pubblicati i risultati.

Questo modello consente ai clienti di adottare la scansione antimalware per i backup senza richiedere le più ampie funzionalità GuardDuty di rilevamento delle minacce, pur fornendo un flusso di lavoro opzionale per l'avvio e la GuardDuty visualizzazione delle operazioni di scansione.

Come funziona la protezione da malware per il backup

Malware Protection for Backup è in grado di eseguire la scansione delle seguenti risorse protette da AWS backup:

- Amazon EBS snapshots
- Amazon EC2 AMIs
- Punti di ripristino Amazon S3
- [Vault bloccati \(immutabili\) \(punti di ripristino EBS/EC2\) che utilizzano Backup AWS Vault Lock nelle regioni supportate](#)

Scansione incrementale

AWS Backup acquisisce le modifiche incrementali per molti tipi di risorse. GuardDuty è in grado di scansionare solo i blocchi o gli oggetti nuovi o modificati al momento della creazione o dell'aggiornamento di un backup, migliorando le prestazioni e riducendo il sovraccarico di scansione e garantendo al contempo una copertura completa nel tempo.

Scansione su richiesta

È possibile avviare una scansione su qualsiasi risorsa di backup supportata in qualsiasi momento, direttamente da AWS Backup o dalla console. GuardDuty I casi d'uso più comuni includono la verifica di un backup prima del ripristino, il ricontrollo dei dati più vecchi dopo la pubblicazione di nuove firme di minaccia o l'esecuzione di scansioni periodiche di conformità.

Note

- La protezione da malware per il backup può essere abilitata solo per le risorse di backup nella stessa regione.
- GuardDuty esegue la scansione di una copia di sola lettura del backup; non modifica il contenuto del backup.
- La scansione funziona sia per gli archivi standard che per gli archivi bloccati (immutabili).

Come funziona Malware Protection for Backup?

Questa sezione descrive i componenti di Malware Protection for Backup, come funziona e come esaminare lo stato e i risultati della scansione del malware.

Panoramica di

Malware Protection for Backup è una funzionalità che consente di rilevare la presenza di malware su istantanee EBS, immagini EC2 (AMI) e punti di ripristino appartenenti ai tipi di risorse EBS, EC2 e S3. Puoi avviare una scansione antimalware su richiesta tramite la GuardDuty console o l'API trasferendo un ruolo IAM che fornisce le autorizzazioni necessarie per la scansione, insieme a una o due risorse a seconda della categoria di scansione. ARNs Sono possibili due categorie di scansione: scansioni complete e scansioni incrementali.

Scansione completa e scansione incrementale

Una scansione completa consente all'API di accettare una risorsa ARN e di scansionare tutti i file all'interno di tale risorsa. Una scansione incrementale invece prende due risorse ARNs, entrambe appartenenti alla stessa risorsa, e analizza i file modificati tra di loro. Ad esempio, supponiamo di scattare un'istantanea di un volume EBS. Chiamiamolo snapshot-1. Se viene eseguita una scansione completa su questa istantanea, GuardDuty analizza tutti i file contenuti in questa istantanea. Supponiamo ora che alcuni file siano stati aggiunti allo stesso volume e che venga scattata una nuova istantanea. Chiamiamolo snapshot-2. Poiché sono stati modificati solo pochi file tra snapshot-1 e snapshot-2, è possibile attivare una scansione incrementale con la risorsa di queste due istantanee. ARNs In questo caso snapshot-2 viene definita risorsa e snapshot-1 viene definita risorsa. *target* base Vedrete questa terminologia usata nel resto del documento. Questa scansione incrementale analizzerà i file modificati tra snapshot-1 e snapshot-2.

Nuova scansione di file precedentemente infetti in una scansione incrementale

Come parte di una scansione incrementale, GuardDuty eseguirà anche una nuova scansione dei file precedentemente infetti dalla scansione di base per un massimo di 365 giorni.

Requisiti per una scansione incrementale

È necessario soddisfare i seguenti requisiti per GuardDuty eseguire una scansione incrementale. Se uno di questi requisiti non viene soddisfatto, GuardDuty salterà la scansione.

- La risorsa di base deve essere analizzata negli ultimi 365 giorni e il risultato della scansione deve essere in COMPLETED o. COMPLETED_WITH_ISSUES

- La risorsa di base deve avere una data di creazione precedente a quella della risorsa di destinazione.
- Le risorse di base e di destinazione devono avere lo stesso tipo di crittografia in caso di istantanee.
- Le risorse di base e di destinazione devono appartenere allo stesso lignaggio.
 - Per uno snapshot EBS e un punto di ripristino EBS, ciò significa che provengono dallo stesso volume o da copie dello stesso volume, senza alcuna modifica del tipo di crittografia.
 - Per un punto di ripristino S3, la risorsa di base e quella di destinazione ARNs devono essere create dallo stesso bucket S3 sottostante.
 - In caso di AMIs, vengono confrontate coppie di istantanee tra l'AMI di base e quella di destinazione per identificare le istantanee per una scansione incrementale. Ogni coppia di istantanee deve soddisfare le condizioni sopra menzionate. Qualsiasi istantanea all'interno dell'AMI di destinazione che non ha un'istantanea corrispondente nell'AMI di base verrà ignorata.

Nuova scansione delle risorse di backup precedentemente scansionate

È possibile avviare una nuova scansione antimalware su richiesta sulla stessa risorsa dopo 10 minuti dall'ora di inizio della scansione antimalware precedente. Se la nuova scansione antimalware viene avviata entro 10 minuti dall'avvio della scansione antimalware precedente, la richiesta genererà il seguente errore e non verrà generato alcun ID di scansione per questa richiesta. I passaggi per ripetere la scansione dell'istanza rimangono gli stessi dell'avvio di una scansione antimalware su richiesta per la prima volta.

Ruolo IAM richiesto per la scansione

È necessario assegnare un ruolo IAM per avviare una scansione completa o incrementale. Questo ruolo fornisce le autorizzazioni necessarie per eseguire le operazioni di scansione. [GuardDuty Protezione da malware per il backup: autorizzazioni IAM Role](#) fornisce l'elenco esatto delle autorizzazioni richieste, insieme alla politica di attendibilità pertinente necessaria per eseguire la scansione.

Revisione dello stato e dei risultati della scansione delle risorse

GuardDuty pubblica l'evento del risultato della scansione sul bus eventi EventBridge predefinito di Amazon. GuardDuty utilizza at-least-once la consegna, il che significa che potresti ricevere più risultati di scansione per lo stesso oggetto. Consigliamo di progettare le applicazioni in modo da gestire risultati duplicati. Ti viene addebitata una sola volta per ogni oggetto scansionato.

Per ulteriori informazioni, consulta [Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for Backup](#).

Revisione dei risultati generati

La revisione dei risultati dipende dal fatto che si stia utilizzando o meno Malware Protection for Backup con GuardDuty. Considerare i seguenti scenari:

Utilizzo di Malware Protection for Backup quando il GuardDuty servizio è abilitato (ID del rilevatore)

Se la scansione antimalware rileva un file potenzialmente dannoso in una risorsa di Backup scansionata, GuardDuty genererà un risultato associato. È possibile visualizzare i dettagli del risultato e utilizzare i passaggi consigliati per correggere potenzialmente il risultato. In base alla [frequenza dei risultati delle esportazioni](#), i risultati generati vengono esportati in un bucket S3 e in un bus di eventi Amazon EventBridge .

Per informazioni sul tipo di risultato che verrebbe generato, vedere [Tipi di ricerca di Malware Protection for Backup](#) Ricerca dei tipi per Malware Protection for Backup.

Utilizzo di Malware Protection for Backup come funzionalità indipendente (nessun ID del rilevatore)

GuardDuty non sarà in grado di generare risultati perché non esiste un ID del rilevatore associato. Per conoscere lo stato della scansione della risorsa di backup, è possibile visualizzare il risultato della scansione che GuardDuty viene pubblicato automaticamente sul bus degli eventi predefinito.

Per informazioni sullo stato e sui risultati della scansione, vedere [Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for Backup](#).

Note

Se utilizzi anche Malware Protection for S3, esiste la possibilità che il tuo file S3 sia stato precedentemente etichettato come NO_THREATS_FOUND e tuttavia lo stesso file possa apparire nell'elenco delle minacce per il Backup Recovery Point a cui appartiene l'oggetto. Ciò accade poiché il servizio aggiorna frequentemente le firme relative ai malware, il che potrebbe aver modificato lo stato del file. Tieni presente che in questi casi GuardDuty non torna indietro e aggiorna il tag sul file nel bucket S3 originale. L'unico modo per applicare un tag aggiornato al file è ricaricare l'oggetto nel bucket o utilizzare la funzione di scansione su richiesta per S3.

GuardDuty Protezione da malware per il backup: autorizzazioni IAM Role

Ruolo del cliente fornito per la scansione del malware

GuardDuty Malware Protection prevede che venga fornito un ruolo al cliente (ruolo scanner) quando vengono avviate le scansioni sulle risorse di Backup, vale a dire istantanee, AMI e 3 punti di ripristino. EBS/EC2/S Questo ruolo fornisce le autorizzazioni necessarie GuardDuty per eseguire la scansione su quelle risorse specifiche. La politica delle autorizzazioni e la politica di fiducia per questo ruolo sono disponibili in: [Autorizzazioni e politica di fiducia per il ruolo](#) La sezione seguente descrive il motivo per cui ciascuna di queste autorizzazioni è richiesta.

Dettagli sulle autorizzazioni

- **ModifySnapshotAttribute**- Consente l'accesso alle istantanee crittografate non crittografate e gestite dal cliente all'account del servizio GuardDuty Malware Protection.
- **CreateGrant**- Consente a GuardDuty Malware Protection di creare e accedere a un volume EBS crittografato con chiave gestita dal cliente a partire dall'istananea crittografata con chiave gestita dal cliente a cui l'account di GuardDuty servizio ha accesso.
- **RetireGrant**- Consente a GuardDuty Malware Protection di ritirare le sovvenzioni create sulla Customer Managed Key per la lettura di istantanee crittografate
- **ReEncryptTo** **ReEncryptFrom** - Richiesto da EBS per GuardDuty consentire l'accesso alle istantanee crittografate con chiavi gestite dal cliente e per creare volumi crittografati a partire da esse. Sebbene i clienti possano considerare ReEncryption un'istananea durante la condivisione come una transizione fondamentale, le istantanee rimangono immutabili dal punto di vista del cliente una volta create.
- **ListSnapshotBlock** **GetSnapshotBlock** - EBS Direct APIs vengono utilizzati per accedere ai blocchi di snapshot per un'istananea crittografata con Managed Key. AWS Ciò avviene perché altrimenti non è possibile accedere alle istantanee crittografate con AWS Managed Key su più account.
- **Decrypt**- Consente di decrittografare le istantanee di base crittografate con chiave gestita dal cliente quando vengono scaricate in memoria utilizzando EBS Direct APIs come parte della scansione incrementale.
- **ListChangedBlocks**- L'API EBS Direct utilizzata nella scansione incrementale delle istantanee per ottenere l'elenco dei blocchi modificati tra due istantanee.

- **DescribeKey**- Consente a GuardDuty Malware Protection di determinare il KeyID della chiave AWS gestita nell'account del cliente.
- **DescribeImages**- Consente di descrivere un AMI per ottenere l'elenco delle istantanee appartenenti all'AMI.
- **DescribeRecoveryPoint**- Consente al servizio di recuperare i dettagli del punto di ripristino e di verificare il tipo di risorsa per il punto di ripristino.
- **CreateBackupAccessPoint, DescribeBackupAccessPoint, DeleteBackupAccessPoint** - Consente al servizio di creare, descrivere ed eliminare l'Access Point necessario per accedere ai punti di ripristino.
- **kms:Decrypt**- Consente al servizio di accedere agli oggetti in un punto di ripristino S3 durante una scansione del punto di ripristino S3.

Garantire il ruolo

Il ruolo deve essere configurato con una politica di fiducia che consideri attendibile il responsabile del servizio GuardDuty Malware Protection. Ciò garantisce che nessun responsabile diverso dal GuardDuty servizio possa assumere questo ruolo. Inoltre, ti consigliamo di limitare le politiche a risorse specifiche anziché*. Ciò include gli ID delle istantanee e gli ID delle chiavi. In questo modo si assicurerà che il ruolo fornisca l'accesso solo a quelle risorse specifiche.

Important

Una configurazione errata potrebbe causare errori di scansione a causa di autorizzazioni insufficienti.

In che modo GuardDuty Malware Protection utilizza le sovvenzioni in KMS AWS

GuardDuty Malware Protection richiede [concessioni](#) per utilizzare le chiavi KMS.

Quando avvii una scansione su un'istananea crittografata o su un'AMI EC2 composta da istantanee crittografate, GuardDuty Malware Protection crea concessioni per tuo conto inviando una [CreateGrant](#) richiesta a KMS. AWS Queste concessioni danno GuardDuty accesso a una chiave specifica del tuo account.

GuardDuty Malware Protection richiede la concessione dell'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia [DescribeKey](#) richieste AWS a per recuperare i dettagli sulla chiave simmetrica gestita dal cliente con cui è crittografata la risorsa inviata per una scansione antimalware.
- Crea un volume EBS da un'istantanea crittografata utilizzando l'[CreateVolume](#) API e crittografa il volume con la stessa chiave.
- Accedi ai blocchi di snapshot sull'istantanea tramite l'[GetSnapshotBlock](#) API durante una scansione incrementale.
- Invia le richieste [Decrypt](#) a AWS KMS per decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per leggere i dati sull'istantanea durante la scansione.

Puoi revocare la concessione creata o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. Se lo fai, non GuardDuty sarai in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da tali dati.

GuardDuty Contesto di crittografia della protezione da malware

Un [contesto di crittografia](#) è un set facoltativo di coppie chiave-valore che contengono ulteriori informazioni contestuali sui dati.

Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS; associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

GuardDuty Malware Protection utilizza uno dei due contesti di crittografia.

Contesto di crittografia 1: La chiave è `aws:guardduty:id`.

```
"encryptionContext": {  
  "aws:guardduty:id": "snap-11112222333344"  
}
```

Questo contesto di crittografia viene utilizzato con le operazioni di concessione: `CreateGrant`, `Decrypt`, `GenerateDataKeyWithoutPlaintext`, `ReEncryptTo`, `RetireGrant`, `DescribeKey`.

Viene creata una concessione sulla risorsa corrente con questo contesto di crittografia e queste operazioni di concessione.

Contesto di crittografia 2: la chiave è `aws:ebs:id`

```
"encryptionContext": {  
  "aws:ebs:id": "snap-11112222333344"  
}
```

Questo contesto di crittografia viene utilizzato con le operazioni di concessione: `ReEncryptFrom`, `Decrypt`, `RetireGrant`. `DescribeKey`

Con questi contesti di crittografia e operazioni di concessione vengono create tre concessioni. Una sull'istantanea di destinazione con l'operazione di concessione. `ReEncryptFrom` Una seconda sull'istantanea di destinazione con `Decrypt`, `RetireGrant`, `DescribeKey` operazioni. E una terza sull'istantanea di base con le stesse operazioni di concessione della seconda concessione.

Autorizzazioni e politica di fiducia per il ruolo

Politica sulle autorizzazioni

```
{  
  "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"
            }
        }
    }
]
}

```

Politica di fiducia

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

```
}  
]  
}
```

(Facoltativo) Inizia a usare Malware Protection for Backup Independently (solo console)

Utilizza questo passaggio facoltativo per iniziare a utilizzare l'opzione di rilevamento delle minacce di Malware Protection for Backup indipendentemente dallo GuardDuty stato del tuo AWS account.

Se desideri utilizzare anche altri piani di protezione dedicati GuardDuty, devi iniziare con il GuardDuty servizio Amazon. Per informazioni sui piani di GuardDuty protezione, consulta [Caratteristiche di GuardDuty](#).

Passaggi per iniziare a usare Malware Protection for Backup

1. Accedi alla console di AWS gestione e apri la <https://console.aws.amazon.com/guardduty/console> all'indirizzo <https://console.aws.amazon.com/guardduty/>
2. Seleziona Discover Malware Protection Features e fai clic su Inizia.
3. Facendo clic su Inizia, puoi scegliere tra opzioni tra cui le funzionalità di AWS Backup e 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](#)

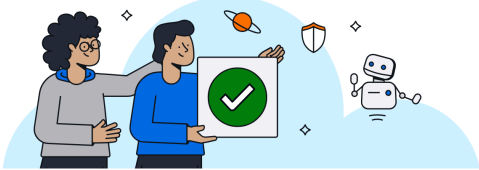
Status

⊖ Not enabled

[View feature](#)

4. Verrai indirizzato alla pagina Malware Protection for Backup, dove puoi scegliere di Avviare una scansione su richiesta o Visualizza le scansioni malware.

Malware Protection for AWS Backup - new [Info](#)
[AWS Service Terms for GuardDuty Malware Protection](#) will apply. Malware detection from scanning cost will apply. [View pricing](#)



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](#)
[Start with AWS Backup](#)

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](#)

Avvio di una scansione su richiesta per la protezione da malware per il backup

Console

1. Accedi alla console di AWS gestione e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Vai a Malware Protection for Backup e fai clic su Avvia scansione su richiesta.
3. Scegli tra Scansione completa e Scansione incrementale.
 1. Per avviare una scansione completa, inserire l'ARN della risorsa da scansionare.
 2. Per una scansione incrementale, immettere Target Resource ARN e Baseline Resource ARN.
 3. Se la risorsa da scansionare è un punto di ripristino, è necessario inserire anche il nome del AWS Backup Vault a cui appartiene.
4. Accesso al servizio: è necessario scegliere un ruolo con le autorizzazioni necessarie per accedere alla risorsa ed eseguire la scansione. Fai clic su Visualizza politica per visualizzare le autorizzazioni esatte necessarie per il ruolo, insieme alla politica di fiducia richiesta.

Puoi apportare modifiche alla politica in base ai tuoi requisiti o limitare le autorizzazioni alla risorsa esatta. Per maggiori dettagli su come creare o aggiornare un ruolo IAM, consulta [GuardDuty Protezione da malware per il backup: autorizzazioni IAM Role](#).

Per problemi con le autorizzazioni dei ruoli IAM, consulta [Risoluzione dell'errore relativo alle autorizzazioni dei ruoli IAM](#).

API/CLI

Invoke [StartMalwareScan](#) che accetta la resourceArn risorsa per la quale si desidera avviare una scansione antimalware su richiesta. Se vuoi avviare una scansione incrementale, esegui l'operazione. `baselineResourceArn incrementalScanDetails` Come parte della configurazione della scansione, devi anche fornire un ruolo IAM con tutte le autorizzazioni necessarie per avviare la scansione. Dopo aver avviato correttamente una scansione, `StartMalwareScan` restituisce `unscanId`. Richiama `GetMalwareScanAPI` per monitorare lo stato di avanzamento della scansione avviata e per ottenere i dettagli della scansione una volta completata.

Monitoraggio degli stati e dei risultati delle scansioni in Malware Protection for Backup

Dopo l'avvio di una scansione antimalware, GuardDuty fornisce alcuni meccanismi attraverso i quali è possibile monitorare lo stato e il risultato di una scansione. La tabella seguente fornisce alcuni dei valori associati alle scansioni antimalware.

Valori potenziali

`RUNNING`, `COMPLETED` , `COMPLETED_WITH_ISSUES` , `FAILED` oppure `SKIPPED`

`FULL_SCAN` o `INCREMENTAL_SCAN`

`GUARDDUTY_INITIATED` , `ON_DEMAND` o `BACKUP_INITIATED`

Valori potenziali

NO_THREATS_FOUND o THREATS_FOUND

*Si noti che lo stato del risultato della scansione potrebbe non essere presente se la scansione non è stata completata. Lo stato del risultato della scansione di THREATS_FOUND indica che è stata GuardDuty rilevata la presenza di malware.

Per i punti di ripristino S3, COMPLETED_WITH_ISSUES indica che alcuni file sono stati ignorati o non sono riusciti. Per gli AMI, COMPLETED_WITH_ISSUES indica che non è stato possibile scansionare almeno 1 istantanea. Di seguito è riportato l'elenco dei motivi ignorati.

Le scansioni possono anche essere ignorate per vari motivi. La tabella seguente spiega i motivi per cui le scansioni possono essere ignorate:

Motivo

Customer Role non dispone delle autorizzazioni necessarie per consentire al servizio di eseguire la scansione

La risorsa che sta tentando di scansionare non esiste nell'account o è stata eliminata durante la scansione

La dimensione dell'istantanea è maggiore di quella attualmente supportata da GuardDuty

Le risorse specificate nella richiesta di scansione incrementale non hanno differenze

Motivo

Risorsa non nello stato previsto. Se la scansione è incrementale, il punto di ripristino di base non è nello stato DISPONIBILE o COMPLETATO

Per le scansioni incrementali: la risorsa di base e quella corrente non provengono dalla stessa discendenza

Per le scansioni incrementali: la risorsa di base non è stata analizzata in precedenza o non è stata trovata alcuna scansione completata

Per le scansioni incrementali, la data di creazione della risorsa di base è maggiore della data di creazione della risorsa corrente

Il tipo di risorsa richiesto non supporta la scansione incrementale

Le AMI pubbliche, le AMI con solo storage temporaneo e le AMI che non sono in uno stato disponibile non sono idonee alla scansione

Le istantanee di conservazione a freddo non sono idonee per la scansione

La scansione non è supportata per i tipi di risorse composite

Motivo

La risorsa richiesta contiene un codice prodotto Amazon Marketplace che non supporta la scansione

Le AMI non supportano la scansione di più di 40 istantanee

Nessuna mappatura dei dispositivi a blocchi Ebs trovata per la risorsa richiesta

Per le scansioni incrementali, l'arn della risorsa di base è diverso dall'arn della risorsa prevista

Tutti i file della scansione sono stati ignorati o non sono riusciti

I risultati della scansione hanno un periodo di conservazione di 90 giorni. Scegli il metodo di accesso che preferisci per monitorare lo stato della scansione malware.

Monitoraggio delle scansioni tramite la console

1. [Apri la GuardDuty console all'indirizzo `https://console.aws.amazon.com/guardduty/`.](https://console.aws.amazon.com/guardduty/)
2. Nel riquadro di navigazione, scegli Scansioni malware.
3. Puoi filtrare le scansioni antimalware in base alle seguenti proprietà disponibili nella barra di ricerca dei filtri.
 - Scan ID: identificatore univoco associato alla scansione antimalware.
 - ID account: account in cui è stata avviata la scansione antimalware.

- ARN della risorsa: Amazon Resource Name (ARN) associato alla risorsa Amazon associata alla scansione.
- Tipo di risorsa: il tipo di risorsa associata alla scansione, ad esempio EC2 Instance, EBS Snapshot | EC2 AMI, EBS Recovery Point, EC2 Recovery Point o S3 Recovery Point.
- Stato: lo stato della scansione, ad esempio Esecuzione, Ignorata, Completata, Completata con problemi o Non riuscita.
- Tipo di scansione: indica se si tratta di una scansione GuardDuty antimalware su richiesta, avviata o avviata da backup.

Monitoraggio delle scansioni tramite l'API/CLI

- È possibile richiamare ListMalwareScans per filtrare le scansioni antimalware con RESOURCE_ARN,,,SCAN_ID, ACCOUNT_ID e. SCAN_TYPE GUARDDUTY_FINDING_ID SCAN_STATUS RESOURCE_TYPE SCAN_START_TIME Puoi anche richiamare GetMalwareScan per recuperare metadati più dettagliati di una scansione fornendo uno scan-id come input. I criteri di GUARDDUTY_FINDING_ID filtro sono disponibili quando viene avviato il. SCAN_TYPE GuardDuty
- È possibile modificare l'esempio *filter-criteria* nel comando seguente e filtrare in base CriterionKey a uno alla volta. Le opzioni per CriterionKey sono Resource_ARNSCAN_ID,ACCOUNT_ID,SCAN_TYPE, GUARDDUTY_FINDING_IDSCAN_STATUS,RESOURCE_TYPE, eSCAN_START_TIME. È possibile modificare *max-results* (fino a 50) e*sort-criteria*. Il AttributeName campo è obbligatorio per sort-criteria e deve essere impostato su scanStartTime. Nell'esempio seguente, i valori in *red* sono segnaposto. Sostituiscili con i valori appropriati per il tuo account. Se usi lo stesso di CriterionKey seguito per ListMalwareScans, assicurati di sostituire l'esempio EqualsValue con quello in base al quale *resource-type* desideri filtrare.

```
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 risposta al comando precedente ListMalwareScans restituirà fino a 25 scansioni con alcuni dettagli sulle risorse interessate. La risposta al comando precedente GetMalwareScan restituirà una singola scansione con metadati dettagliati sulla scansione.

Monitoraggio delle scansioni utilizzando EventBridge

Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, applicazioni Software-as-a-Service (SaaS) e servizi Amazon e indirizza tali dati verso destinazioni come Lambda. In questo modo puoi monitorare gli eventi che si verificano nei servizi e creare architetture basate su eventi. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

GuardDuty pubblica EventBridge le notifiche sul bus degli eventi predefinito una volta determinato lo stato della scansione. Puoi configurare EventBridge regole nel tuo account per inviare eventi ad altri servizi integrati con Amazon EventBridge. Verranno applicati EventBridge i prezzi standard. Per ulteriori informazioni, consulta i [EventBridge prezzi di Amazon](#).

Molti dei valori mostrati di seguito sono segnaposto per l'esempio e variano a seconda della scansione.

Eventi relativi ai risultati della scansione di malware

Potenziali valori del tipo di dettaglio per Backup:

- «Risultato della scansione istantanea EBS di protezione da GuardDuty malware»
- «Risultato della scansione dell'AMI EC2 per la protezione da GuardDuty malware»
- «Risultato della scansione del punto di ripristino di GuardDuty Malware Protection S3»
- «Risultato della scansione del punto di ripristino EBS GuardDuty Malware Protection»
- «Risultato della scansione del punto di ripristino EC2 di protezione da GuardDuty malware»

Esempio di modello di evento:

```
{
  "detail-type": ["GuardDuty Malware Protection EC2 AMI Scan Result"],
  "source": ["aws.guardduty"]
}
```

Schema di notifica di esempio per la scansione dell'AMI EC2 senza minacce rilevate:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",

```

```

    "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": "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
      }
    }
  }
}

```

Schema di notifica di esempio per la scansione dell'AMI EC2 con minacce rilevate:

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "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": "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"
          }
        }]
      }
    }
  }
}

```

Schema di notifica di esempio per la scansione AMI EC2 ignorata:

```

{
  "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
    }
  }
}

```

Quote per la protezione da malware per il backup

Protezione da malware per quote di Backup

Nome quota	AWS valore di quota predefinito	È regolabile?	Description
StartMalwareScan Limite TPS per tutti i tipi di risorse	10	No	
Dimensione massima delle istantanee supportate	2 TB	No	
File system supportati per istantanee e scansioni AMI	- New Technology File System (NTFS) - X File System (XFS) - File System second	No	

Nome quota	AWS valore di quota predefinito	È regolabile?	Description
	extended (ext2) - File System fourth extended (ext4) - File system File Allocation Table (FAT) - File system Virtual File Allocation Table (VFAT)		
Numero massimo di istantanee all'interno di un'AMI supportato per la scansione di malware	40 per la scansione completa. Se ce ne sono più di 40, GuardDuty scansionerà solo 40 tra tutte le istantanee. Per una scansione incrementale, la scansione viene ignorata.	No	

Nome quota	AWS valore di quota predefinito	È regolabile?	Description
Dimensione massima di un oggetto all'interno di un punto di ripristino S3	100 GB	No	La dimensione massima dell'oggetto S3 che GuardDuty tenterà di eseguire la scansione alla ricerca di malware. Sebbene questa quota non sia regolabile, se devi scansionare oggetti più grandi, contatta l'assistenza per determinare se è GuardDuty possibile aumentare la quota per il tuo caso d'uso.
Byte di archivio estratti	100 GB	No	La quantità massima di dati che è GuardDuty possibile estrarre e analizzare da un file di archivio. GuardDuty salterà l'estrazione dei file di archivio per una dimensione superiore a 100 GB.

Nome quota	AWS valore di quota predefinito	È regolabile?	Description
Byte di archivio estratti	10.000	No	Il numero massimo di file che è GuardDuty possibile estrarre e analizzare in un file di archivio. Se l'archivio contiene più di 10.000 file, GuardDuty sarà necessario saltare il file archiviato.  Note I tipi di file composti sono potenzialmente soggetti a questi limiti. I tipi di file includono, a titolo esemplificativo, messaggi di posta elettronica codificati MIME (Multipurpose Internet Mail Extensions), file Compiled Python (PYC), file CHM (Compiled HTML Help), tutti i programmi di installazione e documenti Format (ODF). OpenDocument
Livelli massimi di profondità di archiviazione	5	No	I livelli massimi di archivi annidati che è GuardDuty possibile estrarre. Se l'archivio include file nidificati oltre questo valore, GuardDuty ignorerà tali file nidificati.

GuardDuty Protezione RDS

[RDS Protection in Amazon GuardDuty analizza e profila l'attività di accesso RDS per potenziali minacce di accesso ai tuoi database Amazon Aurora \(Amazon Aurora MySQL Compatible Edition e Aurora PostgreSQL Compatible Edition\) e Amazon RDS for PostgreSQL.](#)

RDS Protection ti aiuta a identificare comportamenti di accesso potenzialmente sospetti su questi database supportati. GuardDuty monitora e profila continuamente le attività [Attività di accesso RDS](#) anomale. Ad esempio, un attore esterno invisibile in precedenza ha accesso non autorizzato al database oppure un avversario tenta di accedere con forza bruta indovinando la password del database.

Con il lancio di [Amazon Aurora PostgreSQL Limitless Database](#), GuardDuty espande RDS Protection per supportare ora anche il monitoraggio delle attività di accesso da Limitless Databases. Per Account AWS questo hanno già abilitato RDS Protection, GuardDuty inizieranno automaticamente a monitorare i dati di accesso dai rispettivi database Limitless. Per gli account che non hanno ancora abilitato la protezione RDS, puoi saperne di più [30-day free trial](#) e scegliere di abilitare questa funzionalità. Per abilitare questa funzionalità, consulta [Abilitazione della protezione RDS in ambienti con più account](#) o [Attivazione della protezione RDS per un account autonomo](#).

Nota

Le istanze di replica di lettura RDS per PostgreSQL richiedono che l'istanza del database principale si trovi su una versione del database supportata e che venga replicata correttamente dal database primario. Per informazioni sulle repliche di lettura, consulta [Working with DB Instance read replicas](#) nella Amazon RDS User Guide.

La Protezione RDS non richiede un'infrastruttura aggiuntiva ed è progettata in modo da non influire negativamente sulle prestazioni delle istanze di database. Quando RDS Protection rileva un tentativo di accesso potenzialmente sospetto o anomalo, ne GuardDuty genera uno o più [Tipi di esiti della Protezione RDS](#) con dettagli sul database potenzialmente compromesso.

Prova gratuita di 30 giorni

- Quando lo abiliti GuardDuty Account AWS in una nuova regione per la prima volta, ricevi una prova gratuita di 30 giorni. In questo caso, GuardDuty abiliterà anche la protezione RDS,

inclusa nella versione di prova gratuita. RDS Protection inizierà a monitorare il comportamento di accesso del database.

- Se lo utilizzi già GuardDuty e decidi di abilitare la protezione RDS in una nuova regione per la prima volta, il tuo account in questa regione riceverà una prova gratuita di 30 giorni per RDS Protection.
- Se hai già abilitato la protezione RDS, con il lancio di [Amazon Aurora PostgreSQL Limitless Database](#), inizierà automaticamente a monitorare l'attività di accesso per i GuardDuty database Limitless. Se la prova gratuita di 30 giorni di RDS Protection è già scaduta, inizierai a incorrere in costi di utilizzo legati al monitoraggio di Limitless Databases.
- Puoi scegliere di disabilitare la protezione RDS in qualsiasi regione e in qualsiasi momento.
- Durante la prova gratuita di 30 giorni, puoi ottenere una stima dei costi di utilizzo per quell'account e per quella regione. Al termine della prova gratuita di 30 giorni, la protezione RDS non viene disattivata automaticamente. Il tuo account in questa regione inizierà a incorrere in costi di utilizzo. Per ulteriori informazioni, consulta [Monitoraggio GuardDuty dell'utilizzo e stima dei costi](#).

Quando la funzionalità di protezione RDS non è abilitata, GuardDuty non rileva comportamenti di accesso anomali o sospetti. Se disabiliti RDS Protection, interrompe GuardDuty immediatamente il monitoraggio dell'attività di accesso RDS e non rileva alcuna potenziale minaccia per le istanze di database supportate né genera tipi di risultati associati.

[Per sapere Regioni AWS dove sono supportati i database Aurora PostgreSQL Limitless, consulta Requisiti per il database Aurora PostgreSQL Limitless.](#)

Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati

La tabella seguente mostra le versioni dei database Aurora e Amazon RDS supportate per RDS Protection.

Amazon Aurora e motore Amazon RDS DB	Versioni del motore supportate
Aurora MySQL	• 2.10.2 o versioni successive • 3.02.1 o versioni successive

Amazon Aurora e motore Amazon RDS DB	Versioni del motore supportate
Aurora PostgreSQL	• 10.23 o versione successiva • 11.12 o versioni successive • 12.7 o versioni successive • 13.3 o versioni successive • 14.3 o versioni successive • 15.2 o versione successiva • 16.1 o versione successiva
RDS per PostgreSQL	• 11.17 o versione successiva • 12.12 o versione successiva • 13.8 o versione successiva • 14.5 o versione successiva • RDS per PostgreSQL versione 15 • RDS per PostgreSQL versione 16 • RDS per PostgreSQL versione 17 • RDS per PostgreSQL versione 18
Database Amazon Aurora PostgreSQL Limitless	16.4-limitless

Attività di accesso RDS

Quando abiliti la funzionalità RDS Protection, avvia GuardDuty automaticamente il monitoraggio dell'attività di accesso RDS per i tuoi database, direttamente dai servizi Aurora e Amazon RDS. L'attività di accesso RDS registra sia i tentativi di accesso riusciti che quelli non riusciti effettuati nel tuo ambiente. [Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati](#) AWS Se esiste un'indicazione di un comportamento di accesso anomalo, GuardDuty genera un risultato con dettagli sul database potenzialmente compromesso. Quando si abilita la protezione RDS per la prima volta o si dispone di un'istanza di database appena creata, è previsto un periodo di apprendimento per definire come base il comportamento normale. Per questo motivo, alle istanze di database appena abilitate o appena create potrebbero non essere associati risultati di accesso anomali per un massimo di due settimane.

Quando RDS Protection rileva una potenziale minaccia, ad esempio uno schema insolito in una serie di tentativi di accesso riusciti, falliti o incompleti, ne genera uno o più. GuardDuty [Tipi di esiti della Protezione RDS](#) In base al tipo di risultato, può includere dettagli sul comportamento anomalo, ad esempio. [Anomalie basate sull'attività di accesso RDS](#)

GuardDuty non gestisce la tua attività di accesso [Database supportati](#) o quella di RDS, né ti rende disponibile l'attività di accesso RDS.

Abilitazione della protezione RDS in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare la funzionalità di protezione RDS per gli account dei membri dell'organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Questo account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio delle attività di accesso RDS per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta. [Account multipli in GuardDuty](#)

Attivazione della protezione RDS per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per configurare il monitoraggio delle attività di accesso RDS per l'account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel riquadro di navigazione, scegli Protezione RDS.
3. Nella pagina Protezione RDS, scegli Modifica.
4. Esegui una delle seguenti operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Scegli Save (Salva).

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Scegli Save (Salva).

API/CLI

Esegui l'operazione [updateDetector](#) API utilizzando il tuo ID di rilevamento regionale e passando l'featuresoggetto di tanto in name tantoRDS_LOGIN_EVENTS. status ENABLED

In alternativa, puoi utilizzare AWS CLI per abilitare la protezione RDS. Esegui il comando seguente e sostituiscilo `12abc34d567e8fa901bc2d34e56789f0` con l'ID del rilevatore del tuo account e `us-east-1` con la regione in cui desideri abilitare la protezione RDS.

Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Abilitare automaticamente la Protezione RDS per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare la funzionalità di Protezione RDS per tutti gli account membri, inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

Utilizzando la pagina Protezione RDS

1. Nel riquadro di navigazione, scegli Protezione RDS.
2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente la Protezione RDS per gli account dell'organizzazione esistenti e per quelli nuovi.
3. Scegli Save (Salva).

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio delle attività di accesso RDS.
4. Scegli Save (Salva).

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta [Abilita selettivamente la protezione RDS per gli account dei membri](#).

API/CLI

Per abilitare o disabilitare in modo selettivo la protezione RDS per i tuoi account membro, richiama l'operazione [updateMemberDetectors](#) API utilizzando la tua *detector ID*

In alternativa, puoi utilizzare AWS CLI per abilitare la protezione RDS. Esegui il comando seguente e sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione RDS.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui l'[ListDetectors](#) API.

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare la Protezione RDS per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare la Protezione RDS per tutti gli account membri attivi esistenti dell'organizzazione. Gli account membri che sono già GuardDuty abilitati vengono definiti membri attivi esistenti.

Console

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, scegli Protezione RDS.
3. Nella pagina Protezione RDS, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

Esegui l'operazione [updateMemberDetectors](#) API utilizzando le tue *detector ID*

In alternativa, puoi utilizzare AWS CLI per abilitare la protezione RDS. Esegui il comando seguente e sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione RDS.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente la Protezione RDS per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare l'attività di accesso RDS per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare nuovi account membro in un'organizzazione tramite la console, utilizzando la pagina Protezione RDS o Account.

Per abilitare automaticamente la Protezione RDS per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

- Utilizzando la pagina Protezione RDS:

1. Nel riquadro di navigazione, scegli Protezione RDS.
2. Nella pagina Protezione RDS, scegli Modifica.
3. Scegli Configura gli account manualmente.
4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione RDS per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.

5. Scegli Save (Salva).

- Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio delle attività di accesso RDS.
4. Scegli Save (Salva).

API/CLI

Per abilitare o disabilitare in modo selettivo la protezione RDS per gli account dei membri, richiama l'operazione [UpdateOrganizationConfiguration](#) API utilizzando la tua *detector ID*

In alternativa, puoi utilizzare AWS CLI per abilitare la protezione RDS. Esegui il comando seguente e sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione RDS. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `autoEnable` su `NONE`.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita selettivamente la protezione RDS per gli account dei membri

Scegli il tuo metodo di accesso preferito per abilitare in modo selettivo il monitoraggio dell'attività di accesso RDS per gli account dei membri.

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

Nella pagina Account, consulta la colonna Attività di accesso RDS per visualizzare lo stato del tuo account membro.

3. Per abilitare o disabilitare in modo selettivo l'attività di accesso RDS

Seleziona l'account per il quale desideri configurare la Protezione RDS. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli Attività di accesso RDS, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo la protezione RDS per i tuoi account membro, richiama l'operazione [updateMemberDetectors](#) API utilizzando la tua. *detector ID*

In alternativa, puoi utilizzare AWS CLI per abilitare la protezione RDS. Esegui il comando seguente e sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione RDS.

Per trovare il codice detectorId relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui l'[ListDetectors](#) API.

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

Note

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Attivazione della protezione RDS per un account autonomo

A un account autonomo spetta la decisione di abilitare o disabilitare un piano di protezione in uno specifico account Account AWS . Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione della protezione RDS in ambienti con più account](#).

Dopo aver abilitato la protezione RDS, GuardDuty inizierà [Attività di accesso RDS](#) il monitoraggio dei database supportati nel tuo account.

Scegli il tuo metodo di accesso preferito per configurare RDS Protection per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel riquadro di navigazione, scegli Protezione RDS.
3. La pagina Protezione RDS mostra lo stato attuale del tuo account. Scegli Abilita per abilitare la protezione RDS.
4. Scegli Conferma per salvare la selezione.

API/CLI

Esegui l'operazione [updateDetector](#)API utilizzando il tuo ID di rilevamento regionale e passando l'featuresoggetto di name tanto `RDS_LOGIN_EVENTS` in status tanto `ENABLED`.

In alternativa, puoi utilizzare AWS CLI per abilitare la protezione RDS. Esegui il comando seguente e sostituiscilo `12abc34d567e8fa901bc2d34e56789f0` con l'ID del rilevatore del tuo account e `us-east-1` con la regione in cui desideri abilitare la protezione RDS.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/>console o esegui l'[ListDetectors](#)API.

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

Risoluzione dei problemi di monitoraggio di RDS Protection

GuardDuty RDS Protection analizza e profila l'attività di accesso RDS per potenziali minacce di accesso a [Database supportati](#). Per raccogliere in modo efficace i dati di telemetria di sicurezza, è GuardDuty necessario che il database sia configurato e funzioni senza problemi. Se il database non è configurato correttamente o presenta problemi, il monitoraggio della sicurezza potrebbe risentirne.

La sezione seguente fornisce i problemi più comuni e i passaggi per risolverli.

Archiviazione RDS completa

Quando l'istanza RDS esaurisce lo spazio di archiviazione, GuardDuty potrebbe non raccogliere dati di telemetria di sicurezza. Il raggiungimento dell'allocazione della capacità di archiviazione dell'istanza DB (`storage-full`) è uno stato critico e RDS consiglia di risolvere immediatamente questo problema. Per ulteriori informazioni, consulta [Visualizzazione dello stato dell'istanza](#) nella Amazon RDS User Guide.

Per risolvere lo `storage-full` stato, puoi eseguire una delle seguenti azioni:

- Abilita la scalabilità automatica dello storage (consigliato): abilita la scalabilità automatica dello storage Amazon RDS per gestire automaticamente la capacità di storage e prevenire condizioni future. `storage-full` Per ulteriori informazioni, consulta [Gestire la capacità automaticamente con Amazon RDS Storage Autoscaling nella Amazon RDS User Guide](#).
- Monitora l'utilizzo dello storage: verifica l'utilizzo dello storage utilizzando uno dei seguenti metodi:
 - Utilizza le CloudWatch metriche per visualizzare i dettagli sullo spazio di archiviazione. Per ulteriori informazioni, consulta [CloudWatch Database Insights](#) nella Amazon CloudWatch User Guide.
 - Visualizza i parametri di storage seguendo i passaggi in [Monitora i parametri in un'istanza Amazon RDS nella Amazon RDS User Guide](#).
- Modifica della capacità di storage: per informazioni sull'aumento della capacità di storage dell'istanza, consulta [Increasing DB Instance Storage Capacity](#) nella Amazon RDS User Guide.

Versioni non supportate sul database primario per RDS per PostgreSQL

Le istanze di replica di lettura RDS per PostgreSQL richiedono che l'istanza del database principale sia nella versione del database supportata e che venga replicata correttamente dal database primario. GuardDuty monitora le istanze solo quando questi requisiti sono soddisfatti.

Per risolvere il problema relativo alla versione non supportata, esegui una delle seguenti operazioni:

- Verifica la compatibilità delle versioni del database: verifica che il tuo database RDS per PostgreSQL primario esegua una delle versioni supportate. Per ulteriori informazioni, consulta [Database supportati](#).
- Risoluzione di un potenziale problema di replica: esamina e risolvi eventuali problemi di replica tra istanze primarie e di replica. Per ulteriori informazioni su questa operazione, consulta [Working with read replicas for RDS for PostgreSQL nella Amazon RDS User Guide](#).

Ulteriori considerazioni sulla sicurezza

Se la tua organizzazione ha requisiti di conformità rigorosi, ti consigliamo di implementare il controllo del database oltre a utilizzare RDS Protection. Per ulteriori informazioni sulle tue responsabilità in materia di sicurezza e sul modello di responsabilità condivisa, consulta [la sezione Security in Amazon RDS](#) nella Amazon RDS User Guide.

GuardDuty Protezione Lambda

La Protezione Lambda è utile per identificare potenziali minacce alla sicurezza quando una funzione [AWS Lambda](#) viene richiamata nel tuo ambiente AWS . Quando abiliti Lambda Protection, GuardDuty inizia a monitorare i registri delle attività di rete Lambda. Ciò include [Log di flusso VPC](#) tutte le funzioni Lambda per il tuo account (compresi i log che non utilizzano la rete VPC) e i log che vengono generati quando viene richiamata la funzione Lambda. Quando GuardDuty identifica un traffico di rete sospetto che è indicativo della presenza di un codice potenzialmente dannoso nella funzione Lambda, GuardDuty ne genera uno o più. [Tipi di esiti della Protezione Lambda](#)

Prova gratuita di 30 giorni

L'elenco seguente spiega come funziona la prova gratuita di 30 giorni per il tuo account:

- Quando la attivi GuardDuty Account AWS in una nuova regione per la prima volta, ricevi una prova gratuita di 30 giorni. In questo caso, GuardDuty abiliterà anche la protezione Lambda, inclusa nella versione di prova gratuita.
- Se utilizzi già Lambda Protection GuardDuty e decidi di abilitare Lambda Protection per la prima volta, il tuo account in questa regione riceverà una prova gratuita di 30 giorni per Lambda Protection.
- Puoi scegliere di disabilitare la protezione Lambda in qualsiasi regione in qualsiasi momento.
- Durante la prova gratuita di 30 giorni, puoi ottenere una stima dei costi di utilizzo per quell'account e per quella regione. Al termine della prova gratuita di 30 giorni, Lambda Protection non viene disabilitata automaticamente. Il tuo account in questa regione inizierà a incorrere in costi di utilizzo. Per ulteriori informazioni, consulta [Monitoraggio GuardDuty dell'utilizzo e stima dei costi](#).

I registri delle attività di rete Lambda sono soggetti a modifiche, inclusa l'espansione ad altre attività di rete come i dati delle query DNS generati richiamando le funzioni Lambda. L'espansione ad altre forme di monitoraggio delle attività di rete aumenterà il volume di dati che GuardDuty verranno elaborati per Lambda Protection. il che avrà un impatto diretto sul costo di utilizzo di questa protezione. Ogni volta che GuardDuty inizia a monitorare un registro delle attività di rete aggiuntivo, fornirà un avviso agli account che hanno attivato Lambda Protection, almeno 30 giorni prima del rilascio.

 Note

Il monitoraggio delle attività di rete Lambda non include i log per le [funzioni Lambda @Edge](#).

Monitoraggio delle attività di rete Lambda

Quando abiliti Lambda Protection, GuardDuty monitora i registri delle attività di rete Lambda che vengono generati quando viene richiamata una funzione Lambda associata al tuo account. Ciò consente di rilevare potenziali minacce alla sicurezza della funzione Lambda. Per le funzioni Lambda configurate per utilizzare la rete VPC, non è necessario abilitare i log di flusso VPC per le interfacce di rete elastiche (ENI) create da Lambda for. GuardDuty addebita solo la quantità di dati dei registri delle attività di rete Lambda elaborati (in GB) per generare un risultato. GuardDuty ottimizza i costi applicando filtri intelligenti e analizzando un sottoinsieme di registri delle attività di rete Lambda rilevanti per il rilevamento delle minacce.

GuardDuty non gestisce i registri delle attività della rete Lambda (inclusi i log di flusso VPC e non VPC) né li rende accessibili nel tuo account.

Abilitazione della protezione Lambda in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare Lambda Protection per gli account dei membri della propria organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. L'account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio dell'attività di rete Lambda per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta [Gestione di più account in Amazon](#). GuardDuty

Attivazione di Lambda Protection per l'account amministratore delegato GuardDuty

Scegli il tuo metodo di accesso preferito per abilitare o disabilitare il monitoraggio dell'attività di rete Lambda per l'account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

2. Nel riquadro di navigazione, in Impostazioni, scegli Protezione Lambda.
3. Nella pagina Protezione Lambda, scegli Modifica.
4. Esegui una delle seguenti operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Scegli Save (Salva).

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Scegli Save (Salva).

API/CLI

Esegui l'operazione [updateDetector](#) API utilizzando il tuo ID di rilevamento regionale e passando l'feature soggetto di tanto in nome tanto LAMBDA_NETWORK_LOGS. status ENABLED

In alternativa, è possibile utilizzare AWS CLI per abilitare la protezione Lambda. Esegui il comando seguente e sostituiscilo `12abc34d567e8fa901bc2d34e56789f0` con l'ID del rilevatore del tuo account e `us-east-1` con la regione in cui desideri abilitare la protezione Lambda.

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Abilitare automaticamente il monitoraggio delle attività di rete Lambda per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare la funzionalità di monitoraggio delle attività di rete Lambda per tutti gli account membri, inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

Utilizzando la pagina Protezione Lambda

1. Nel riquadro di navigazione, scegli Protezione Lambda.
2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente il monitoraggio delle attività di rete Lambda per gli account dell'organizzazione esistenti e per quelli nuovi.
3. Scegli Save (Salva).

Note

L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio delle attività di rete Lambda.

 Note

Per impostazione predefinita, questa azione attiva automaticamente l'opzione Attivazione automatica GuardDuty per nuovi account membro.

4. Scegli Save (Salva).

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta [Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri](#).

API/CLI

Per abilitare o disabilitare selettivamente il monitoraggio dell'attività di rete Lambda per i tuoi account membro, richiama l'operazione API [updateMemberDetectors](#) utilizzando la tua *detector ID*

In alternativa, è possibile utilizzare AWS CLI per abilitare la protezione Lambda. Esegui il comando seguente e sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione Lambda.

Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui 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"}]'
```

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti dell'organizzazione.

Console

Per configurare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, scegli Protezione Lambda.
3. Nella pagina Protezione Lambda, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

Per abilitare o disabilitare selettivamente il monitoraggio dell'attività di rete Lambda per i tuoi account membro, richiama l'operazione API [updateMemberDetectors](#) utilizzando la tua *detector ID*

In alternativa, è possibile utilizzare AWS CLI per abilitare la protezione Lambda. Esegui il comando seguente e sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione Lambda.

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente il monitoraggio delle attività di rete Lambda per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio delle attività di rete Lambda per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare il monitoraggio dell'attività di rete Lambda per i nuovi account membro di un'organizzazione, utilizzando la pagina Lambda Protection o Account.

Per abilitare automaticamente il monitoraggio delle attività di rete Lambda per i nuovi account membri

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una delle seguenti operazioni:

- Utilizzando la pagina Protezione Lambda:

1. Nel riquadro di navigazione, scegli Protezione Lambda.
2. Nella pagina Protezione Lambda, scegli Modifica.
3. Scegli Configura gli account manualmente.
4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione Lambda per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
5. Scegli Save (Salva).

- Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.

3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio delle attività di rete Lambda.
4. Scegli Save (Salva).

API/CLI

Per abilitare il monitoraggio dell'attività di rete Lambda per i nuovi account membro, richiama l'operazione [UpdateOrganizationConfiguration](#) API utilizzando la tua *detector ID*

In alternativa, è possibile utilizzare AWS CLI per abilitare la protezione Lambda. L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione Lambda. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `AutoEnable` su `NONE`.

Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere Accounts (Account).

Nella pagina Account, consulta la colonna Monitoraggio delle attività di rete Lambda, che indica se il monitoraggio delle attività di rete Lambda è abilitato o meno.

3. Scegli l'account per il quale desideri configurare la Protezione Lambda. Puoi scegliere più account alla volta.
4. Dal menu a discesa Modifica piani di protezione, scegli Monitoraggio delle attività di rete Lambda, quindi scegli l'operazione appropriata.

API/CLI

Invoca l'[updateMemberDetectors](#)API usando le tue. *detector ID*

In alternativa, è possibile utilizzare AWS CLI per abilitare la protezione Lambda. Sostituiscilo *12abc34d567e8fa901bc2d34e56789f0* con l'ID del rilevatore del tuo account e *us-east-1* con la regione in cui desideri abilitare la protezione Lambda.

Per trovare l'indirizzo detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#)API.

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di UnprocessedAccounts. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Attivazione di Lambda Protection per un account autonomo

A un account autonomo spetta la decisione di abilitare o disabilitare un piano di protezione in uno specifico account Account AWS . Regione AWS

Se il tuo account è associato a un account GuardDuty amministratore tramite AWS Organizations o tramite il metodo di invito, questa sezione non si applica al tuo account. Per ulteriori informazioni, consulta [Abilitazione della protezione Lambda in ambienti con più account](#).

Dopo aver abilitato Lambda Protection, GuardDuty inizierà il monitoraggio [Monitoraggio delle attività di rete Lambda](#) nel tuo account.

Scegli il tuo metodo di accesso preferito per configurare Lambda Protection per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel riquadro di navigazione, in Impostazioni, scegli Protezione Lambda.
3. La pagina della Protezione Lambda mostra lo stato attuale del tuo account. Scegli Abilita per abilitare Lambda Protection nel tuo account.
4. Scegli Conferma per salvare la selezione.

API/CLI

Esegui l'operazione [updateDetector](#) API utilizzando il tuo ID di rilevamento regionale e passando l'feature soggetto di nome tanto LAMBDA_NETWORK_LOGS in status tanto ENABLED.

In alternativa, è possibile utilizzare AWS CLI per abilitare la protezione Lambda. Esegui il comando seguente e sostituiscilo `12abc34d567e8fa901bc2d34e56789f0` con l'ID del rilevatore del tuo account e `us-east-1` con la regione in cui desideri abilitare la protezione Lambda.

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

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

Protezione dei carichi di lavoro AI con GuardDuty

Amazon GuardDuty [Foundational Threat Detection](#) e [Lambda](#) Protection ti aiutano a proteggere e rilevare meglio le minacce ai carichi di lavoro di intelligenza artificiale su cui si basano. AWS

[Il rilevamento fondamentale delle GuardDuty minacce monitora gli eventi di AWS CloudTrail gestione per rilevare attività sospette e dannose nei carichi di lavoro di intelligenza artificiale generativa creati utilizzando servizi AWS , tra cui Amazon Bedrock e Amazon AI. SageMaker](#) Ad esempio, può identificare attività come GuardDuty :

- Rimozione insolita dei parapetti di sicurezza di Amazon Bedrock
- Modifica della fonte dei dati di addestramento del modello che può potenzialmente portare a un attacco di data poisoning
- Richiamata sospetta del modello Amazon Bedrock
- Registrazione disattivata per le chiamate del modello Amazon Bedrock che possono indicare tentativi di eludere il rilevamento
- Istanza insolita di un notebook o creazione di posti di formazione nell'intelligenza artificiale SageMaker
- Credenziali Amazon Elastic Compute Cloud esfiltrate che potrebbero essere state utilizzate per richiamare APIs Amazon Bedrock, Amazon SageMaker AI o carichi di lavoro AI autogestiti su EC2 istanze, cluster EKS o attività ECS.

GuardDuty Lambda Protection può aiutare a rilevare potenziali minacce legate agli agenti Amazon Bedrock. Ciò può includere attività di rete sospette, come il cryptomining, e la comunicazione con server di comando e controllo malevoli, che possono essere causate da attacchi alla catena di fornitura o richieste complesse.

Il video seguente mostra come apparirebbero i risultati associati.

Il video seguente mostra come apparirebbero i risultati associati. [Utilizzo GuardDuty di Amazon per monitorare e proteggere i carichi di lavoro di intelligenza artificiale basati su AWS](#)

Account multipli in Amazon GuardDuty

Se AWS l'ambiente dispone di più account, è possibile gestirli designandone uno Account AWS come account amministratore. È quindi possibile associare i multipli Account AWS a questo account amministratore come account membro. Con questa configurazione, un account GuardDuty amministratore designato può valutare e monitorare la sicurezza generale dell'organizzazione. L'account amministratore può anche eseguire attività di gestione degli account, come la revisione di tutti i risultati generati e la configurazione dei piani di protezione interni GuardDuty.

In GuardDuty, un'organizzazione è composta da un account GuardDuty amministratore delegato e da uno o più account membro associati. È possibile associare gli account in due modi: mediante l'integrazione o utilizzando un metodo legacy di invio e accettazione degli inviti di iscrizione nella console. AWS Organizations GuardDuty GuardDuty consiglia l'integrazione con. AWS Organizations

AWS Organizations è un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire centralmente più account. Account AWS Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più piattaforme Servizi AWS, tra cui Macie e Amazon. AWS Security Hub CSPM GuardDuty Per ulteriori informazioni, consulta la [Guida per l'utente AWS Organizations](#).

Indice

- [Comprensione della relazione tra account GuardDuty amministratore e account membro](#)
- [Gestione GuardDuty degli account con AWS Organizations](#)
- [Gestione GuardDuty degli account su invito](#)
- [GuardDuty considerazioni sull'esportazione dei dettagli dell'account membro in formato CSV](#)

Comprensione della relazione tra account GuardDuty amministratore e account membro

Quando si utilizza GuardDuty in un ambiente con più account, l'account amministratore può gestire determinati aspetti per GuardDuty conto degli account dei membri. Un account amministratore può svolgere le seguenti funzioni principali:

- Aggiungere e rimuovere account membri associati: il processo con cui un account amministratore può eseguire questa operazione varia in base al modo in cui gestisci gli account, tramite AWS Organizations o tramite il metodo di GuardDuty invito.

GuardDuty consiglia di gestire gli account dei membri tramite AWS Organizations.

- Attivazione GuardDuty dell'account amministratore delegato GuardDuty nell'account di gestione: se l'account di AWS Organizations gestione viene disabilitato GuardDuty, l'account GuardDuty amministratore delegato può attivarsi GuardDuty nell'account di gestione. Tuttavia, è necessario che l'account di gestione non abbia eliminato in modo esplicito il [Autorizzazioni di ruolo collegate al servizio per GuardDuty](#)
- Configura lo stato degli account dei membri: un account amministratore può abilitare o disabilitare lo stato dei piani di GuardDuty protezione e abilitare, sospendere o disabilitare lo stato di per GuardDuty conto degli account dei membri associati.

GuardDuty L'account amministratore delegato gestito con AWS Organizations può essere abilitato automaticamente GuardDuty quando Account AWS vengono aggiunti come membri.

- Personalizza quando generare i risultati: un account amministratore può personalizzare i risultati all'interno della GuardDuty rete creando e gestendo regole di soppressione, elenchi di IP affidabili ed elenchi di minacce. In un ambiente con più account, il supporto per la configurazione di queste funzionalità è disponibile solo per un account amministratore delegato. GuardDuty Un account membro non può aggiornare questa configurazione.

La tabella seguente descrive in dettaglio la relazione tra account GuardDuty amministratore e account membro.

Chiave per la tabella

- Autonomo: un account può eseguire l'azione elencata solo per il proprio account.
- Qualsiasi: un account può eseguire l'azione elencata per qualsiasi account associato.
- Tutti: un account può eseguire l'azione elencata e questa si applica a tutti gli account associati. In genere, l'account che esegue questa azione è un account GuardDuty amministratore designato
- Celle con trattino (—) — Le celle della tabella con trattino (—) indicano che l'account non può eseguire l'azione elencata.

Azione

Tramite AWS Organizations

Su invito

	Account GuardDuty amministratore delegato	Account membro associato	GuardDuty account amministratore	Account membro associato
Abilita GuardDuty	Qualsiasi	–	Personale	Personale
Abilita GuardDuty automaticamente per l'intera organizzazione (ALL,NEW,NONE)	Tutti	–	–	–
Visualizza tutti gli account dei membri di Organizat ions indipende ntemente GuardDuty dallo stato	Qualsiasi	–	–	–
Genera risultati di esempio	Personale	Personale	Personale	Personale
Visualizza tutti i GuardDuty risultati	Qualsiasi	Personale	Qualsiasi	Personale
Archivia GuardDuty i risultati	Qualsiasi	–	Qualsiasi	–
Applica regole di soppressione	Tutti	–	Tutti	–

Crea un elenco di IP o elenchi di minacce affidabili	Tutti	–	Tutti	–
Aggiorna l'elenco di IP attendibili o gli elenchi di minacce	Tutti	–	Tutti	–
Eliminare l'elenco di IP attendibili o gli elenchi di minacce	Tutti	–	Tutti	–
Imposta la frequenza di EventBridge notifica	Tutti	–	Tutti	–
Imposta la posizione Amazon S3 per l'esportazione degli esiti	Tutti	Personale	Personale	Personale
Abilita uno o più piani di protezione e opzionali per l'intera organizzazione (ALL,NEW,NONE)	Tutti	–	–	–
Questo non include Malware Protection for S3.				

Abilita qualsiasi piano di GuardDuty protezione per i singoli account	Qualsiasi	–	Qualsiasi	–
Ciò non include Malware Protection for EC2 e Malware Protection for S3.				
Protezione da malware per EC2	Qualsiasi	–	Personale	–
Protezione da malware per EC2: scansione antimalware su richiesta	Qualsiasi	Personale	Personale	Personale
Protezione da malware per S3	–	Personale	–	Personale
Annulla l'associazione di un account membro	Qualsiasi +	–	Qualsiasi	–
Dissociarsi da un account amministratore	–	–	–	Personale
Eliminare un account membro dissociato	Qualsiasi	–	Qualsiasi	–
Sospendere GuardDuty	Qualunque *	–	Qualunque *	–

Disabilita GuardDuty	Qualunque *	–	Qualunque *	Personale

⁺ Indica che l'account GuardDuty amministratore delegato può eseguire questa azione solo se non ha impostato le preferenze di attivazione automatica per i membri ALL dell'organizzazione.

^{*} Indica che un account GuardDuty amministratore delegato non può essere disattivato direttamente GuardDuty in un account membro. L'account GuardDuty amministratore delegato deve prima dissociare l'account membro e quindi eliminarlo. Dopodiché, ogni account membro può essere disattivato GuardDuty nei propri account. Per ulteriori informazioni sull'esecuzione di queste attività nella propria organizzazione, vedere [Gestione continua degli account dei membri all'interno GuardDuty](#).

Gestione GuardDuty degli account con AWS Organizations

In un' AWS organizzazione, l'account di gestione può designare qualsiasi account all'interno di questa organizzazione come account amministratore delegato. GuardDuty Per questo account amministratore, GuardDuty viene abilitato automaticamente solo nell'account corrente. Regione AWS Per impostazione predefinita, l'account amministratore può abilitare e gestire tutti GuardDuty gli account dei membri dell'organizzazione all'interno di quella regione. L'account amministratore può visualizzare e aggiungere membri a questa AWS organizzazione.

Le seguenti sezioni illustreranno le varie attività che è possibile eseguire come account GuardDuty amministratore delegato.

Indice

- [Considerazioni e consigli per l'utilizzo con GuardDuty AWS Organizations](#)
- [Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty](#)
- [Designazione di un account amministratore delegato GuardDuty](#)
- [Impostazione delle preferenze di attivazione automatica dell'organizzazione](#)
- [Aggiungere membri all'organizzazione](#)
- [\(Facoltativo\) Abilita i piani di protezione per gli account dei membri esistenti](#)
- [Gestione continua degli account dei membri all'interno GuardDuty](#)
- [Sospensione GuardDuty per l'account di un membro](#)

- [Dissociazione \(rimozione\) dell'account membro dall'account amministratore](#)
- [Eliminazione degli account dei membri dall'organizzazione GuardDuty](#)
- [Modifica dell' GuardDuty account amministratore delegato](#)

Considerazioni e consigli per l'utilizzo con GuardDuty AWS Organizations

Le considerazioni e i consigli seguenti possono aiutarti a capire come funziona un account GuardDuty amministratore delegato in: GuardDuty

Un account GuardDuty amministratore delegato può gestire un massimo di 50.000 membri.

È previsto un limite di 50.000 account membro per account amministratore delegato GuardDuty . Ciò include gli account membro aggiunti tramite AWS Organizations o quelli che hanno accettato l'invito dell'account GuardDuty amministratore a entrare a far parte della propria organizzazione. Tuttavia, nella tua AWS organizzazione potrebbero esserci più di 50.000 account.

Se superi il limite di 50.000 account membri, riceverai una notifica e un'e-mail all'account amministratore delegato designato GuardDuty . CloudWatch Health Dashboard

Un account GuardDuty amministratore delegato è regionale.

Al contrario AWS Organizations, GuardDuty è un servizio regionale. Gli account di GuardDuty amministratore delegato e i relativi account membro devono essere aggiunti AWS Organizations in ogni regione desiderata in cui è stata GuardDuty abilitata. Se l'account di gestione dell'organizzazione designa un account GuardDuty amministratore delegato solo negli Stati Uniti orientali (Virginia settentrionale), l'account GuardDuty amministratore delegato gestirà solo gli account dei membri aggiunti all'organizzazione in quella regione. Per ulteriori informazioni sulla parità di funzionalità nelle regioni in cui GuardDuty è disponibile, consulta. [Regioni ed endpoint](#)

Casi speciali per le regioni che hanno aderito

- Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (NEW) o su tutti gli account membro (ALL), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della [GuardDuty console](#) o utilizza l'API. [ListMembers](#)
- Quando lavori con la configurazione di GuardDuty attivazione automatica impostata su NEW, assicurati che sia soddisfatta la seguente sequenza:

1. Gli account dei membri aderiscono a una regione opt-in.
2. Aggiungi gli account dei membri alla tua organizzazione in. AWS Organizations

Se modifichi l'ordine di questi passaggi, l'impostazione di GuardDuty attivazione automatica con non **NEW** funzionerà nella regione di attivazione specifica perché l'account membro non è più nuovo per l'organizzazione. GuardDuty offre due soluzioni alternative:

- Imposta la configurazione di GuardDuty attivazione automatica su ALL, che include account membri nuovi ed esistenti. In questo caso, l'ordine di questi passaggi non è rilevante.
- Se un account membro fa già parte della tua organizzazione, gestisci la GuardDuty configurazione di questo account individualmente nella regione di attivazione specifica utilizzando la GuardDuty console o l'API.

È necessario che un' AWS organizzazione disponga dello stesso account GuardDuty amministratore delegato in tutti i. Regioni AWS

È necessario designare un account membro come account GuardDuty amministratore delegato per tutti gli account where abilitati Regioni AWS . GuardDuty Ad esempio, se si designa un account membro **111122223333** in **Europe (Ireland)**, non è possibile designare un altro account membro in. **555555555555** **Canada (Central)** È necessario utilizzare lo stesso account dell'account GuardDuty amministratore delegato in tutte le altre regioni.

È possibile designare un nuovo account GuardDuty amministratore delegato in qualsiasi momento. Per ulteriori informazioni sulla rimozione dell'account GuardDuty amministratore delegato esistente, consulta. [Modifica dell' GuardDuty account amministratore delegato](#)

Non è consigliabile impostare l'account di gestione dell'organizzazione come account GuardDuty amministratore delegato.

L'account di gestione dell'organizzazione può essere l'account GuardDuty amministratore delegato. Tuttavia, le best practice di sicurezza AWS seguono il principio del privilegio minimo e sconsigliano questa configurazione.

La modifica di un account GuardDuty amministratore delegato non disabilita gli account GuardDuty dei membri.

Se rimuovi un account GuardDuty amministratore delegato, GuardDuty rimuove tutti gli account membro associati a tale account amministratore delegato GuardDuty . GuardDuty rimane comunque abilitato per tutti questi account membro.

Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty

Per iniziare a utilizzare Amazon GuardDuty con AWS Organizations, l'account di AWS Organizations gestione dell'organizzazione designa un account come account GuardDuty amministratore delegato. Questo abilita GuardDuty come servizio affidabile in. AWS Organizations Abilita inoltre GuardDuty l'account GuardDuty amministratore delegato e consente inoltre all'account amministratore delegato di abilitare e gestire GuardDuty altri account dell'organizzazione nella regione corrente. Per informazioni su come vengono concesse queste autorizzazioni, vedere [Utilizzo AWS Organizations con](#) altri servizi. AWS

Come account di AWS Organizations gestione, prima di designare l'account GuardDuty amministratore delegato per l'organizzazione, verificate di poter eseguire le seguenti GuardDuty azioni: `guardduty:EnableOrganizationAdminAccount` Questa azione consente di designare l'account GuardDuty amministratore delegato per l'organizzazione utilizzando. GuardDuty È inoltre necessario assicurarsi di avere il permesso di eseguire le AWS Organizations azioni che consentono di recuperare informazioni sulla propria organizzazione.

Per concedere queste autorizzazioni, includi la seguente dichiarazione in una policy AWS Identity and Access Management (IAM) per il tuo account:

```
{
  "Sid": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}
```

Se desideri designare il tuo account di AWS Organizations gestione come account GuardDuty amministratore delegato, il tuo account richiederà anche l'azione IAM:

CreateServiceLinkedRole Questa azione consente di inizializzare l'account GuardDuty di gestione. Tuttavia, controlla [Considerazioni e consigli per l'utilizzo con GuardDuty AWS Organizations](#) prima di procedere con l'aggiunta delle autorizzazioni.

Per continuare a designare l'account di gestione come account GuardDuty amministratore delegato, aggiungi la seguente dichiarazione alla policy IAM e sostituiscila **111122223333** con l' Account AWS ID dell'account di gestione della tua organizzazione:

```
{
  "Sid": "PermissionsToEnableGuardDuty"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "guarddduty.amazonaws.com"
    }
  }
}
```

Designazione di un account amministratore delegato GuardDuty

Questa sezione fornisce i passaggi per designare un amministratore delegato nell'organizzazione. GuardDuty

In qualità di account di gestione dell' AWS organizzazione, assicurati di leggere attentamente come funziona un account GuardDuty amministratore delegato. [Considerazioni e raccomandazioni](#) Prima di procedere, assicurati di averlo fatto. [Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty](#)

Scegliete un metodo di accesso preferito per designare un account GuardDuty amministratore delegato per la vostra organizzazione. Solo un account di gestione può eseguire questo passaggio.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guarddduty/>.

Per accedere, utilizza le credenziali dell'account di gestione della tua AWS Organizations organizzazione.

2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri designare l'account amministratore delegato GuardDuty per la tua organizzazione.
3. Effettua una delle seguenti operazioni, a seconda che GuardDuty sia abilitato per il tuo account di gestione nella regione corrente:
 - Se non GuardDuty è abilitato, seleziona Amazon GuardDuty - tutte le funzionalità e scegli Inizia. Questa azione ti porterà alla GuardDuty pagina Benvenuto.
 - Se GuardDuty è abilitata, scegli Impostazioni nel riquadro di navigazione.
4. In Amministratore delegato, inserisci l' Account AWS ID a 12 cifre dell'account che desideri designare come account GuardDuty amministratore delegato per l'organizzazione.

Assicurati di abilitarlo GuardDuty per il tuo account GuardDuty amministratore delegato appena designato, altrimenti non sarà in grado di intraprendere alcuna azione.

5. Scegli Delega.
6. (Consigliato) Ripeti i passaggi precedenti per designare l'account GuardDuty amministratore delegato in ogni account in Regione AWS cui hai abilitato. GuardDuty

API/CLI

1. Esegui [enableOrganizationAdminAccount](#) utilizzando le credenziali dell'account di gestione Account AWS dell'organizzazione.
 - In alternativa, è possibile utilizzare AWS Command Line Interface per eseguire questa operazione. Il AWS CLI comando seguente designa un account GuardDuty amministratore delegato solo per la regione corrente. Esegui il AWS CLI comando seguente e assicurati di sostituirlo **111111111111** con l' Account AWS ID dell'account che desideri designare come account amministratore delegato GuardDuty :

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

Per designare l'account GuardDuty amministratore delegato per altre regioni, specifica la regione nel comando. AWS CLI L'esempio seguente mostra come abilitare un account

GuardDuty amministratore delegato negli Stati Uniti occidentali (Oregon). Assicurati di sostituirlo *us-west-2* con la regione a cui desideri assegnare l'account amministratore delegato. GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

Per informazioni su Regioni AWS dove GuardDuty è disponibile, consulta. [Regioni ed endpoint](#)

Se GuardDuty è disabilitato per il tuo account GuardDuty amministratore delegato, non sarà in grado di intraprendere alcuna azione. Se non l'hai già fatto, assicurati di abilitarlo GuardDuty per il nuovo GuardDuty account amministratore delegato designato.

2. (Consigliato) Ripeti i passaggi precedenti per designare l'account GuardDuty amministratore delegato in ogni account in Regione AWS cui hai abilitato. GuardDuty

Impostazione delle preferenze di attivazione automatica dell'organizzazione

La funzionalità di attivazione automatica dell'organizzazione GuardDuty consente di impostare lo stesso stato GuardDuty e i piani di protezione per NEW gli account ALL esistenti o membri dell'organizzazione, in un unico passaggio. Allo stesso modo, puoi anche specificare quando non desideri intraprendere alcuna azione sugli account dei membri, NONE selezionando. I passaggi seguenti spiegano queste impostazioni e indicano anche quando si desidera utilizzare un'impostazione specifica.

Note

Puoi impostare le preferenze di attivazione automatica per tutti i piani di protezione tranne [Protezione da malware per S3](#).

Scegli un metodo di accesso preferito per aggiornare le preferenze di attivazione automatica per l'organizzazione.

Console

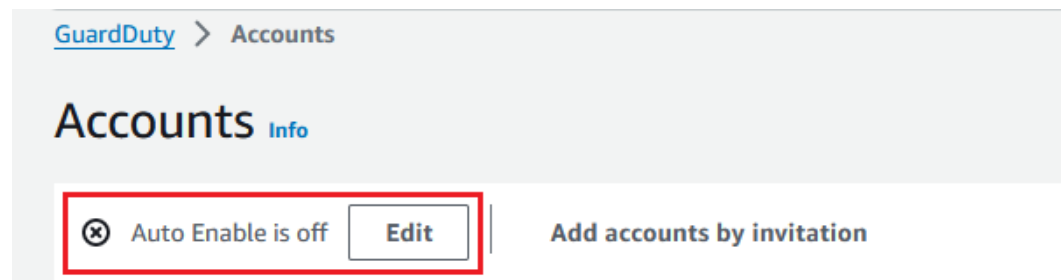
1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Per accedere, utilizza le credenziali GuardDuty dell'account amministratore.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

La pagina Account fornisce opzioni di configurazione per l'account GuardDuty amministratore da abilitare automaticamente GuardDuty e i piani di protezione opzionali per conto degli account membri che appartengono all'organizzazione.

3. Per aggiornare le impostazioni di attivazione automatica esistenti, scegli Modifica.



Questo supporto è disponibile per la configurazione GuardDuty e per tutti i piani di protezione opzionali supportati nel tuo Regione AWS. Puoi selezionare una delle seguenti opzioni di configurazione per GuardDuty conto dei tuoi account membro:

- Abilita per tutti gli account (**ALL**): seleziona questa opzione per abilitare l'opzione corrispondente per tutti gli account di un'organizzazione. inclusi i nuovi account che entrano a far parte dell'organizzazione e gli account che potrebbero essere stati sospesi o rimossi dall'organizzazione. Ciò include anche l'account GuardDuty amministratore delegato.

Note

Potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri.

- Attivazione automatica per nuovi account (**NEW**): seleziona questa opzione per abilitare GuardDuty automaticamente i piani di protezione opzionali solo per i nuovi account membri quando entrano a far parte dell'organizzazione.
- Non abilitare (**NONE**): seleziona questa opzione per impedire l'attivazione dell'opzione corrispondente per i nuovi account dell'organizzazione. In questo caso, l'account GuardDuty amministratore gestirà ogni account singolarmente.

Quando aggiorni l'impostazione di attivazione automatica da ALL o NEW verso NONE, questa azione non disattiva l'opzione corrispondente per i tuoi account esistenti. Questa

configurazione verrà applicata ai nuovi account che entrano a far parte dell'organizzazione. Dopo aver aggiornato le impostazioni di attivazione automatica, nessun nuovo account avrà l'opzione corrispondente abilitata.

Note

Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (NEW) o su tutti gli account membro (ALL), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della [GuardDuty console](#) o utilizza l'API. [ListMembers](#)

4. Scegli Save changes (Salva modifiche).
5. (Facoltativo) se desideri utilizzare le stesse preferenze in ogni regione, aggiorna le preferenze in ciascuna delle regioni supportate separatamente.

Alcuni dei piani di protezione opzionali potrebbero non essere disponibili in tutti i paesi in Regioni AWS cui GuardDuty sono disponibili. Per ulteriori informazioni, consulta [Regioni ed endpoint](#).

API/CLI

1. Esegui [UpdateOrganizationConfiguration](#) utilizzando le credenziali dell'account GuardDuty amministratore delegato, per configurare automaticamente GuardDuty e i piani di protezione opzionali in quella regione per la tua organizzazione. [Per informazioni sulle varie configurazioni di attivazione automatica, vedere autoEnableOrganization Membri](#).

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Per impostare le preferenze di abilitazione automatica per uno qualsiasi dei piani di protezione facoltativi supportati nella tua regione, segui i passaggi riportati nelle sezioni della documentazione corrispondenti a ciascun piano di protezione.

2. Puoi convalidare le preferenze per la tua organizzazione nella regione attuale. Esegui [describeOrganizationConfiguration](#). Assicurati di specificare l'ID del rilevatore dell' GuardDuty account amministratore delegato.

 Note

L'aggiornamento della configurazione per tutti gli account membri può richiedere fino a 24 ore.

3. In alternativa, esegui il AWS CLI comando seguente per impostare le preferenze da abilitare o disabilitare automaticamente GuardDuty in quella regione per i nuovi account (NEW) che entrano a far parte dell'organizzazione, per tutti gli account (ALL) o per nessuno degli account (NONE) dell'organizzazione. Per ulteriori informazioni, consulta [autoEnableOrganizationMembers](#). In base alle tue preferenze, potrebbe essere necessario sostituire NEW con ALL o NONE. Se si configura il piano di protezione con ALL, il piano di protezione verrà abilitato anche per l'account GuardDuty amministratore delegato. Assicurati di specificare l'ID del rilevatore dell'account GuardDuty amministratore delegato che gestisce la configurazione dell'organizzazione.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

4. Puoi convalidare le preferenze per la tua organizzazione nella regione attuale. Esegui il AWS CLI comando seguente utilizzando l'ID del rilevatore dell' GuardDuty account amministratore delegato.

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```

(Consigliato) ripeti i passaggi precedenti in ogni regione utilizzando l'ID del rilevatore dell'account GuardDuty amministratore delegato.

 Note

Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (NEW) o su tutti gli account membro (ALL), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della [GuardDuty console](#) o utilizza l'API. [ListMembers](#)

Aggiungere membri all'organizzazione

Come account GuardDuty amministratore delegato, puoi aggiungerne uno o più Account AWS all' GuardDuty organizzazione. Quando aggiungi un account come GuardDuty membro, questo verrà automaticamente GuardDuty abilitato in quella regione. Esiste un'eccezione relativamente all'account di gestione dell'organizzazione. Prima che l'account dell'account di gestione venga aggiunto come GuardDuty membro, deve essere GuardDuty abilitato.

Scegli un metodo preferito per aggiungere un account membro alla tua GuardDuty organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Per accedere, utilizza le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

La tabella degli account mostra tutti gli account membro attivi (non sospesi Account AWS) e che possono essere associati all'account amministratore delegato GuardDuty . Se l'account membro è associato all'account amministratore dell'organizzazione, il Tipo sarà uno dei seguenti: Tramite Organizations o By invitation. Se un account membro non è associato all'account GuardDuty amministratore dell'organizzazione, il Tipo di account membro è Non un membro.

3. Seleziona uno o più account IDs che desideri aggiungere come membri. Questi account IDs devono avere il tipo come Via Organizations.

Gli account aggiunti tramite invito non fanno parte dell'organizzazione. Puoi gestire tali account singolarmente. Per ulteriori informazioni, consulta [Gestione degli account tramite invito](#).

4. Scegli il menu a discesa Azioni, quindi scegli Aggiungi membro. Dopo aver aggiunto questo account come membro, verrà applicata la GuardDuty configurazione di attivazione automatica. In base alle impostazioni di [Impostazione delle preferenze di attivazione automatica dell'organizzazione](#), la GuardDuty configurazione di questi account potrebbe cambiare.
5. Puoi selezionare la freccia rivolta verso il basso della colonna Stato per ordinare gli account in base allo stato Non sono un membro e quindi scegliere ogni account che non è GuardDuty abilitato nella regione corrente.

Se nessuno degli account elencati nella tabella degli account è stato ancora aggiunto come membro, puoi abilitarlo GuardDuty nella regione corrente per tutti gli account dell'organizzazione. Scegli Abilita nel banner nella parte superiore della pagina. Questa azione attiva automaticamente la GuardDuty configurazione di attivazione automatica in modo che GuardDuty venga abilitata per ogni nuovo account che si unisce all'organizzazione.

6. Scegli Conferma per aggiungere gli account come membri. Questa azione si attiva anche GuardDuty per tutti gli account selezionati. Lo Stato degli account cambia in Abilitato.
7. (Consigliato) Ripeti questi passaggi in ciascuno di essi Regione AWS. Ciò garantisce che l'account GuardDuty amministratore delegato possa gestire i risultati e altre configurazioni per gli account dei membri in tutte le regioni in cui è stata GuardDuty abilitata.

La funzionalità di attivazione automatica abilita tutti GuardDuty i futuri membri della tua organizzazione. Ciò consente GuardDuty all'account amministratore delegato di gestire tutti i nuovi membri creati all'interno o aggiunti all'organizzazione. Quando il numero di account membri raggiunge il limite di 50.000, la funzione di attivazione automatica viene disattivata automaticamente. Se rimuovi un account membro e il numero totale di membri scende a meno di 50.000, la funzione di attivazione automatica si riattiva.

API/CLI

- Esegui [CreateMembers](#) utilizzando le credenziali dell'account amministratore delegato GuardDuty .

È necessario specificare l'ID del rilevatore regionale dell'account GuardDuty amministratore delegato e i dettagli dell'account (Account AWS IDs e gli indirizzi e-mail corrispondenti) degli account che si desidera aggiungere come membri. GuardDuty È possibile creare uno o più membri con questa operazione API.

Quando lavori CreateMembers nella tua organizzazione, le preferenze di attivazione automatica per i nuovi membri verranno applicate quando nuovi account membro entrano a far parte dell'organizzazione. Se utilizzi CreateMembers un account membro esistente, la configurazione dell'organizzazione verrà applicata anche ai membri esistenti. Ciò potrebbe modificare la configurazione attuale degli account dei membri esistenti.

Esegui [ListAccounts](#) nell'AWS Organizations API Reference, per visualizzare tutti gli account dell' AWS organizzazione.

- In alternativa, puoi usare AWS Command Line Interface. Esegui il comando AWS CLI seguente e assicurati di utilizzare il tuo ID rilevatore, l'ID Account AWS e l'indirizzo e-mail validi associati all'ID account.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

Puoi visualizzare un elenco di tutti i membri dell'organizzazione eseguendo il seguente AWS CLI comando:

```
aws organizations list-accounts
```

Dopo aver aggiunto questo account come membro, verrà applicata la GuardDuty configurazione di attivazione automatica.

(Facoltativo) Abilita i piani di protezione per gli account dei membri esistenti

La procedura seguente include i passaggi per abilitare i piani di protezione per gli account dei membri esistenti utilizzando la pagina Account. Per i passaggi da eseguire a tale scopo utilizzando l'API oppure AWS CLI, consulta i documenti relativi al piano di protezione specifico.

Puoi abilitare i piani di protezione per singoli account tramite la pagina Account.

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Utilizza le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona uno o più account per i quali desideri configurare un piano di protezione. Ripeti i seguenti passaggi per ogni piano di protezione da configurare:
 - a. Scegli Modifica piani di protezione.
 - b. Dall'elenco dei piani di protezione, scegli quello da configurare.
 - c. Scegli una delle operazioni che desideri eseguire per questo piano di protezione, quindi scegli Conferma.
 - d. Per l'account selezionato, la colonna corrispondente al piano di protezione configurato mostrerà la configurazione aggiornata come Abilitata o Non abilitata.

Gestione continua degli account dei membri all'interno GuardDuty

In qualità di account GuardDuty amministratore delegato, sei responsabile del mantenimento della configurazione GuardDuty e dei relativi piani di protezione opzionali per tutti gli account dell'organizzazione supportati. Regione AWS Le seguenti sezioni forniscono le opzioni relative al mantenimento dello stato di configurazione GuardDuty o di uno qualsiasi dei relativi piani di protezione opzionali:

Per mantenere lo stato di configurazione dell'intera organizzazione in ogni regione

- Imposta le preferenze di attivazione automatica per l'intera organizzazione utilizzando la GuardDuty console: puoi abilitarla GuardDuty automaticamente per tutti (ALL) i membri dell'organizzazione o per i nuovi (NEW) membri che si uniscono all'organizzazione, oppure scegliere di non (NONE) abilitare automaticamente nessuno dei membri dell'organizzazione.

Puoi anche configurare le stesse impostazioni o impostazioni diverse per tutti i piani di protezione inclusi. GuardDuty

Potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri dell'organizzazione.

- Aggiorna le preferenze di attivazione automatica utilizzando l'API — Run [UpdateOrganizationConfiguration](#)to configura automaticamente GuardDuty e i relativi piani di protezione opzionali per l'organizzazione. Quando corri [CreateMembers](#)ad aggiungere nuovi account membro nella tua organizzazione, le impostazioni configurate verranno applicate automaticamente. Se utilizzi CreateMembers un account membro esistente, la configurazione dell'organizzazione verrà applicata anche ai membri esistenti. Ciò potrebbe modificare la configurazione attuale degli account dei membri esistenti.

Per visualizzare tutti gli account della tua organizzazione, [ListAccounts](#)esegui l'AWS Organizations API Reference.

Per mantenere lo stato di configurazione per i singoli account dei membri in ciascuna regione

- Per visualizzare tutti gli account della tua organizzazione, [ListAccounts](#)esegui l'AWS Organizations API Reference.
- Se desideri che gli account membro selettivi abbiano uno stato di configurazione diverso, esegui l'operazione [UpdateMemberDetectors](#)per ogni account membro singolarmente.

Puoi utilizzare la GuardDuty console per eseguire la stessa operazione accedendo alla pagina Account della console. GuardDuty

Per informazioni sull'attivazione dei piani di protezione per singoli account utilizzando la console o l'API, consulta la pagina di configurazione per il piano di protezione corrispondente.

Sospensione GuardDuty per l'account di un membro

In qualità di account GuardDuty amministratore delegato, puoi sospendere il GuardDuty servizio per un account membro della tua organizzazione. In tal caso, l'account membro rimane nell'organizzazione. GuardDuty Puoi anche riattivarli GuardDuty per questi account membro in un secondo momento. Tuttavia, se alla fine desideri dissociare (rimuovere) questo account membro, dopo aver seguito i passaggi in questa sezione, devi seguire i passaggi indicati in. [Dissociazione \(rimozione\) dell'account membro dall'account amministratore](#)

Quando effettui la sospensione GuardDuty in un account membro, puoi aspettarti le seguenti modifiche:

- GuardDuty non monitora più la sicurezza dell' AWS ambiente né genera nuove scoperte.
- I risultati esistenti nell'account del membro rimangono intatti.
- Un account membro GuardDuty sospeso non comporta alcun addebito per. GuardDuty

Se l'account membro ha abilitato Malware Protection for S3 per uno o più bucket del proprio account, la sospensione GuardDuty non influisce sulla configurazione di Malware Protection for S3. L'account membro continuerà a sostenere i costi di utilizzo di Malware Protection for S3. Affinché l'account membro smetta di utilizzare Malware Protection for S3, deve disabilitare questa funzionalità per i bucket protetti. Per ulteriori informazioni, consulta [Disattivazione di Malware Protection for S3 per un bucket protetto](#).

Scegli un metodo preferito di sospensione GuardDuty per un account membro della tua organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Per accedere, utilizza le credenziali dell' GuardDuty account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, seleziona uno o più account per i quali desideri sospendere. GuardDuty
4. Scegli il menu a discesa Azioni, quindi scegli Sospendi. GuardDuty
5. Scegli Sospendi GuardDuty per confermare la selezione.

Questo cambierà lo stato dell'account del membro in Disabilitato (sospeso).

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui desideri dissociare o rimuovere l'account del membro.

API

1. Per recuperare l'ID dell'account membro per il quale desideri sospendere GuardDuty, utilizza l'API. [ListMembers](#) Includi il `OnlyAssociated` parametro nella tua richiesta. Se si imposta

il valore di questo parametro su `true`, GuardDuty restituisce un `members` array che fornisce dettagli solo sugli account attualmente GuardDuty membri.

In alternativa, puoi usare AWS Command Line Interface (AWS CLI) per eseguire il seguente comando:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Sostituisci *us-east-1* con la regione in cui desideri sospendere GuardDuty per questo account.

2. Per sospendere uno o più account GuardDuty membri, esegui la procedura [StopMonitoringMembers](#) di sospensione GuardDuty per un account membro.

In alternativa, puoi usare AWS CLI per eseguire il seguente comando:

```
aws guardduty stop-monitoring-members --detector-id  
12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Sostituisci *us-east-1* con la regione in cui desideri sospendere questo account. Se hai un elenco di account IDs che desideri rimuovere, separali con uno spazio.

Se desideri ulteriormente dissociare (rimuovere) questo account membro, segui i passaggi indicati [Dissociazione \(rimozione\) dell'account membro dall'account amministratore](#).

Dissociazione (rimozione) dell'account membro dall'account amministratore

Quando desideri interrompere la configurazione delle GuardDuty impostazioni e l'accesso ai dati da un account membro, rimuovi quell'account come account membro GuardDuty . Puoi farlo dissociando (rimuovendo) quell'account dall' GuardDuty account amministratore.

Quando si dissocia un account GuardDuty membro, accade quanto segue:

- GuardDuty rimane abilitato per l'account corrente Regione AWS, ma l'account viene dissociato dall'account amministratore delegato GuardDuty .
- L'account dissociato continua a essere visualizzato nell'inventario dell'account.
- L'account GuardDuty amministratore non ha più accesso ai risultati di questo account autonomo.
- Il proprietario dell'account non viene informato della dissociazione.

Puoi aggiungere nuovamente l'account dissociato alla tua organizzazione in un secondo momento.

Scegli un metodo preferito per dissociare (rimuovere) un account membro dalla tua organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Per accedere, utilizza le credenziali dell' GuardDuty account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella tabella Account, è possibile rimuovere un account con Tipo come Via Organizations e Status as Enabled.

Seleziona uno o più account con lo stesso tipo e stato.

4. Dal menu a discesa Azioni, scegli Dissocia account.
5. Scegli Dissocia account per confermare la selezione.
6. Il valore dello status per gli account selezionati cambierà in Non sono un membro. Il conteggio di Via Organizations (Active/All) nell'angolo in alto a destra della pagina Account cambierà in base all'aggiornamento.

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui desideri dissociare l'account membro.

API

1. Per recuperare l'ID dell'account membro che desideri rimuovere, utilizza l'API. [ListMembers](#) Includi il `OnlyAssociated` parametro nella tua richiesta. Se si imposta il valore di questo parametro su `true`, GuardDuty restituisce un `members` array che fornisce dettagli solo sugli account attualmente GuardDuty membri.

In alternativa, puoi usare AWS Command Line Interface (AWS CLI) per eseguire il seguente comando:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Sostituisci *us-east-1* con la regione in cui desideri rimuovere questo account.

2. Per rimuovere uno o più account GuardDuty membro, esegui [DisassociateMembers](#) per rimuovere l'account membro associato all'account amministratore.

In alternativa, puoi usare AWS CLI per eseguire il seguente comando:

```
aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE  
--account-ids 111122223333 --region us-east-1
```

Sostituisci *us-east-1* con la regione in cui desideri rimuovere questo account. Se hai un elenco di account IDs che desideri rimuovere, separali con uno spazio.

Eliminazione degli account dei membri dall'organizzazione GuardDuty

Come account GuardDuty amministratore delegato, dopo aver dissociato un account membro e non desideri più mantenerlo nell' GuardDuty organizzazione, puoi eliminare quell'account membro dall'organizzazione. GuardDuty Questo account membro non comparirà più nell'inventario del tuo account. Tuttavia, se non GuardDuty è stato sospeso in questo account membro, la configurazione GuardDuty e i piani di protezione dedicati rimangono gli stessi. Questo account diventerà ora un account autonomo e potrà [GuardDutydisattivarsi](#) da solo.

Questo passaggio non eliminerà l'account membro dalla tua AWS organizzazione.

Scegli un metodo preferito per eliminare un account membro dalla tua GuardDuty organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Per accedere, utilizza le credenziali dell' GuardDuty account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella tabella Account, è possibile rimuovere un account con Tipo come Via Organizations e Status as Removed (disassociato).

Seleziona uno o più account con lo stesso tipo e stato.

4. Dal menu a discesa Azioni, scegli Elimina account.
5. Scegli Elimina account per confermare la selezione. Il membro dell'account selezionato non verrà più visualizzato nella tabella Account.

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui desideri eliminare questo account membro.

API/CLI

1. Per recuperare l'ID dell'account membro che desideri eliminare, utilizza l'[ListMembers](#) API. Includi il `OnlyAssociated` parametro nella tua richiesta. Se si imposta il valore di questo parametro su `false`, GuardDuty restituisce un `members` array che fornisce dettagli solo sugli account che attualmente sono GuardDuty membri non associati.

In alternativa, puoi usare AWS Command Line Interface (AWS CLI) per eseguire il seguente comando:

```
aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
```

Sostituiscilo `12abc34d567e8fa901bc2d34EXAMPLE` con l'ID del rilevatore dell'account GuardDuty amministratore delegato e `us-east-1` con la regione in cui desideri rimuovere questo account.

2. Per eliminare uno o più account GuardDuty membro, esegui [DeleteMembers](#) per eliminare l'account membro dall' GuardDuty organizzazione.

In alternativa, puoi usare AWS CLI per eseguire il seguente comando:

```
aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Sostituisci `12abc34d567e8fa901bc2d34EXAMPLE` con l'ID del rilevatore dell'account GuardDuty amministratore delegato e `us-east-1` con la regione in cui desideri rimuovere questo account. Se hai un elenco di account IDs che desideri rimuovere, separali con uno spazio.

Modifica dell' GuardDuty account amministratore delegato

Puoi rimuovere l'account GuardDuty amministratore delegato per la tua organizzazione in ogni regione e quindi delegare un nuovo amministratore in ogni regione. Per mantenere il livello di sicurezza degli account dei membri dell'organizzazione in una regione, è necessario disporre di un account GuardDuty amministratore delegato in quella regione.

 Nota

Prima di rimuovere un account GuardDuty amministratore delegato, è necessario dissociare tutti gli account membro associati all'account GuardDuty amministratore delegato e quindi eliminarli dall'organizzazione. GuardDuty Per ulteriori informazioni su questi passaggi, consulta i seguenti documenti:

- [Dissociazione \(rimozione\) dell'account membro dall'account amministratore](#)
- [Eliminazione degli account dei membri dall'organizzazione GuardDuty](#)

Rimozione dell' GuardDuty account amministratore delegato esistente

Passaggio 1: rimuovere l'account GuardDuty amministratore delegato esistente in ciascuna regione

1. Come account GuardDuty amministratore delegato esistente, elenca tutti gli account membro associati al tuo account amministratore. Esegui [ListMembers](#) con `onlyAssociated=false`.
2. Se la preferenza di attivazione automatica per GuardDuty o per uno qualsiasi dei piani di protezione opzionali è impostata su ALL, esegui [UpdateOrganizationConfiguration](#) per aggiornare la configurazione dell'organizzazione su uno dei due NEW piani di protezione opzionali. NONE Questa azione eviterà che si verifichi un errore quando si dissociano tutti gli account dei membri nel passaggio successivo.
3. Esegui [DisassociateMembers](#) per dissociare tutti gli account membro associati all'account amministratore.
4. Esegui [DeleteMembers](#) per eliminare le associazioni tra l'account amministratore e gli account dei membri.
5. Come account di gestione dell'organizzazione, esegui [DisableOrganizationAdminAccount](#) per rimuovere l'account GuardDuty amministratore delegato esistente.
6. Ripeti questi passaggi in ognuno dei Regione AWS paesi in cui hai questo GuardDuty account amministratore delegato.

Fase 2 - Annullare la registrazione GuardDuty dell'account amministratore delegato esistente in AWS Organizations (azione globale una tantum)

- Esegui [DeregisterDelegatedAdministrator](#) nell'AWS Organizations API Reference, per annullare la registrazione dell'account amministratore delegato GuardDuty esistente in. AWS Organizations

In alternativa, puoi eseguire il seguente AWS CLI comando:

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --service-principal guardduty.amazonaws.com
```

Assicurati di sostituirlo **111122223333** con l'account GuardDuty amministratore delegato esistente.

Dopo aver annullato la registrazione del vecchio account GuardDuty amministratore delegato, puoi aggiungerlo come account membro al nuovo account amministratore delegato GuardDuty .

Designazione di un nuovo account amministratore delegato GuardDuty in ogni regione

- Designate un nuovo account GuardDuty amministratore delegato in ogni regione utilizzando il metodo di accesso preferito: GuardDuty console o API oppure. AWS CLI Per ulteriori informazioni, consulta [Designazione di un account amministratore delegato GuardDuty](#).
- Esegui [DescribeOrganizationConfiguration](#) per visualizzare l'attuale configurazione di attivazione automatica per la tua organizzazione.

Important

Prima di aggiungere membri al nuovo account GuardDuty amministratore delegato, è necessario verificare la configurazione di attivazione automatica per l'organizzazione. Questa configurazione è specifica del nuovo account GuardDuty amministratore delegato e della regione selezionata e non si riferisce a. AWS Organizations Quando si aggiunge un account membro dell'organizzazione (nuovo o esistente) al nuovo account GuardDuty amministratore delegato, la configurazione di attivazione automatica del nuovo account GuardDuty amministratore delegato verrà applicata al momento dell'attivazione GuardDuty o di uno qualsiasi dei suoi piani di protezione opzionali.

Modifica la configurazione dell'organizzazione per il nuovo account GuardDuty amministratore delegato utilizzando il metodo di accesso preferito: GuardDuty console o API o. AWS CLI. Per ulteriori informazioni, consulta [Impostazione delle preferenze di attivazione automatica dell'organizzazione](#).

Gestione GuardDuty degli account su invito

Per gestire gli account esterni all'organizzazione, è possibile utilizzare il metodo di invito legacy. Quando utilizzi questo metodo, il tuo account viene designato come account amministratore nel momento in cui un altro account accetta l'invito a diventare un account membro.

Note

GuardDuty consiglia di utilizzare, AWS Organizations al posto degli GuardDuty inviti, per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione degli account con AWS Organizations](#).

Se il tuo account non è un account amministratore, puoi accettare un invito da un altro account. Quando accetti l'invito, il tuo account diventa un account membro. Un AWS account non può essere contemporaneamente un account GuardDuty amministratore e un account membro.

Quando accetti un invito da un account, non puoi accettare un invito da un altro account. Per accettare un invito da un altro account, devi prima dissociare il tuo account dall'account amministratore esistente. In alternativa, l'account amministratore può anche dissociare e rimuovere il tuo account dalla sua organizzazione.

Gli account associati su invito hanno una account-to-member relazione amministrativa complessiva simile a quella degli account associati da AWS Organizations, come descritto in [Comprensione della relazione tra account GuardDuty amministratore e account membro](#). Tuttavia, gli utenti con account amministratore a inviti non possono GuardDuty attivare gli account dei membri associati o visualizzare altri account non membri all'interno della propria AWS Organizations organizzazione.

Important

Quando si GuardDuty creano account membri utilizzando questo metodo, può verificarsi un trasferimento di dati interregionale. Per verificare gli indirizzi e-mail degli account dei membri,

GuardDuty utilizza un servizio di verifica e-mail che opera solo nella regione degli Stati Uniti orientali (Virginia settentrionale).

Argomenti

- [Aggiungere account su invito](#)
- [Consolidamento degli account degli GuardDuty amministratori in un'unica organizzazione](#)

Aggiungere account su invito

Come account amministratore già GuardDuty abilitato, puoi aggiungere membri per iniziare a utilizzarli GuardDuty. Dopo aver aggiunto i membri, puoi invitarli a partecipare GuardDuty e loro possono scegliere di rispondere al tuo invito.

Note

GuardDuty consiglia di utilizzare, AWS Organizations al posto degli GuardDuty inviti, per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione degli account con AWS Organizations](#).

Scegli un metodo di accesso preferito per aggiungere account GuardDuty membro come account GuardDuty amministratore.

Console

Fase 1: aggiunta di un account

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Scegli Aggiungi account tramite invito nel riquadro superiore.
4. Nella pagina Aggiungi account membri, in Inserisci i dettagli dell'account, inserisci l'ID e l'indirizzo e-mail dell' Account AWS associati all'account che desideri aggiungere.
5. Per aggiungere un'altra riga in cui immettere i dettagli dell'account uno alla volta, scegli Aggiungi un altro account. Puoi anche scegliere Carica il file .csv con i dettagli dell'account per aggiungere account in blocco.

⚠ Important

La prima riga del file csv deve contenere l'intestazione, come illustrato nell'esempio seguente: Account ID,Email. Ogni riga successiva deve contenere un unico Account AWS ID valido e l'indirizzo e-mail associato. Il formato di una riga è valido se contiene un solo ID dell' Account AWS e l'indirizzo e-mail associato separati da una virgola.

Account ID,Email

55555555555, user@example.com

6. Dopo aver aggiunto tutti i dettagli degli account, scegli Successivo. Puoi visualizzare gli account appena aggiunti nella tabella Account. Lo Stato di questi account sarà Invito non inviato. Per informazioni sull'invio di un invito a uno o più account aggiunti, consulta [Step 2 - Invite an account](#).

Fase 2: invito di un account

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona uno o più account che desideri invitare su Amazon GuardDuty.
4. Scegli il menu a discesa Operazioni, quindi Invita.
5. Nella GuardDuty finestra di dialogo Invito a, inserisci un messaggio di invito (opzionale).

Se l'account invitato non ha accesso alla posta elettronica, seleziona la casella di controllo Invia anche una notifica e-mail all'utente root dell'invitato Account AWS e genera un avviso in quello dell'invitato. Dashboard AWS Health

6. Selezionare Send invitation (Invia invito). Se gli invitati hanno accesso all'indirizzo e-mail specificato, possono visualizzare l'invito aprendo la console all'indirizzo. GuardDuty <https://console.aws.amazon.com/guardduty/>
7. Quando un invitato accetta l'invito, il valore nella colonna Stato cambia in Invitato. Per informazioni sull'accettazione di un invito, consulta [Step 3 - Accept an invitation](#).

Fase 3: accettazione di un invito

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

 Important

È necessario abilitarla GuardDuty prima di poter visualizzare o accettare un invito all'iscrizione.

2. Effettua le seguenti operazioni solo se non l'hai GuardDuty ancora abilitato; in caso contrario, puoi saltare questo passaggio e continuare con il passaggio successivo.

Se non l'hai ancora abilitato GuardDuty, scegli Get Started sulla GuardDuty pagina Amazon.

Nella pagina Welcome to GuardDuty (Benvenuto su) scegli Enable GuardDuty (Abilita).

3. Dopo aver attivato GuardDuty il tuo account, segui la procedura seguente per accettare l'invito all'iscrizione:
 - a. Nel pannello di navigazione scegli Impostazioni.
 - b. Scegli Account.
 - c. In Account, assicurati di verificare il proprietario dell'account dal quale accetti l'invito. Attiva Accetta per accettare l'invito.
4. Dopo aver accettato l'invito, il tuo account diventa un account GuardDuty membro. L'account il cui proprietario ha inviato l'invito diventa l'account GuardDuty amministratore. L'account amministratore saprà che hai accettato l'invito. La tabella Account GuardDuty del relativo account verrà aggiornata. Il valore nella colonna Stato corrispondente all'ID del tuo account membro cambierà in Abilitato. Il proprietario dell'account amministratore può ora visualizzare GuardDuty e gestire le configurazioni del piano di protezione per conto del tuo account. L'account amministratore può anche visualizzare e gestire i GuardDuty risultati generati per il tuo account membro.

API/CLI

Puoi designare un account GuardDuty amministratore e creare o aggiungere account GuardDuty membro su invito tramite le operazioni API. Esegui le seguenti operazioni GuardDuty API per designare l'account amministratore e gli account membro in. GuardDuty

Completa la procedura seguente utilizzando le credenziali dell' Account AWS account che desideri designare come amministratore. GuardDuty

Creazione o aggiunta di account membri

1. Esegui l'operazione [CreateMembers](#) API utilizzando le credenziali dell' AWS account abilitato. GuardDuty Questo è l'account che desideri utilizzare come GuardDuty account amministratore.

È necessario specificare l'ID del rilevatore dell' AWS account corrente e l'ID account e l'indirizzo e-mail degli account di cui si desidera diventare GuardDuty membri. È possibile creare uno o più membri con questa operazione API.

Puoi anche utilizzare gli strumenti della riga di AWS comando per designare un account amministratore eseguendo il seguente comando CLI. Assicurati di utilizzare il tuo ID rilevatore valido, l'ID account e l'e-mail.

Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Esegui [InviteMembers](#) utilizzando le credenziali dell' AWS account che hai GuardDuty abilitato. Questo è l'account che desideri utilizzare come GuardDuty account amministratore.

È necessario specificare l'ID del rilevatore dell' AWS account corrente e l'account IDs degli account di cui si desidera diventare GuardDuty membri. È possibile invitare uno o più membri con questa operazione API.

Note

È anche possibile specificare un messaggio di invito facoltativo tramite il parametro di richiesta `message`.

È inoltre possibile AWS Command Line Interface utilizzarlo per designare gli account dei membri eseguendo il comando seguente. Assicurati di utilizzare un ID rilevatore valido e un account valido IDs per gli account che desideri invitare.

Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-ids 111122223333
```

Accettazione degli inviti

Completa la procedura seguente utilizzando le credenziali di ogni AWS account che desideri designare come account GuardDuty membro.

1. Esegui l'operazione [CreateDetectorAPI](#) per ogni AWS account che è stato invitato a diventare un account GuardDuty membro e per il quale desideri accettare un invito.

È necessario specificare se la risorsa del rilevatore deve essere abilitata utilizzando il GuardDuty servizio. Un rilevatore deve essere creato e abilitato per GuardDuty diventare operativo. È necessario abilitarlo GuardDuty prima di accettare un invito.

È inoltre possibile eseguire questa operazione utilizzando gli strumenti della riga di AWS comando utilizzando il seguente comando CLI.

```
aws guardduty create-detector --enable
```

2. Esegui l'operazione [AcceptAdministratorInvitationAPI](#) per ogni AWS account per il quale desideri accettare l'invito all'iscrizione, utilizzando le credenziali di quell'account.

Devi specificare l'ID del rilevatore di questo AWS account per l'account membro, l'ID account dell'account amministratore che ha inviato l'invito e l'ID dell'invito che stai accettando. È possibile trovare l'ID account dell'account amministratore dall'e-mail di invito o utilizzando l'operazione [ListInvitations](#) dell'API.

Puoi anche accettare un invito utilizzando AWS Command Line Tools eseguendo il seguente comando CLI. Assicurati di utilizzare ID rilevatore, ID account amministratore e ID invito validi.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--administrator-id 444455556666 --invitation-  
id 84b097800250d17d1872b34c4daadcf5
```

Consolidamento degli account degli GuardDuty amministratori in un'unica organizzazione

GuardDuty consiglia di utilizzare l'associazione AWS Organizations per gestire gli account dei membri con un account GuardDuty amministratore delegato. È possibile utilizzare il processo di esempio descritto di seguito per consolidare l'account amministratore e il membro associato su invito in un'organizzazione in un unico account amministratore GuardDuty delegato GuardDuty .

Note

GuardDuty consiglia di utilizzare, AWS Organizations al posto degli GuardDuty inviti, per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione degli account con AWS Organizations](#).

Gli account che sono già gestiti da un account GuardDuty amministratore delegato o gli account dei membri attivi associati all'account GuardDuty amministratore delegato non possono essere aggiunti a un altro account amministratore delegato GuardDuty . Ogni organizzazione può avere un solo account GuardDuty amministratore delegato per regione e ogni account membro può avere un solo account amministratore delegato. GuardDuty

Scegli un metodo di accesso preferito per consolidare gli account GuardDuty amministratore in un unico account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>

Per accedere, utilizza le credenziali dell'account di gestione dell'organizzazione.

2. Tutti gli account che desideri gestire GuardDuty devono far parte della tua organizzazione. Per informazioni sull'aggiunta di un account alla tua organizzazione, vedi [Invitare un utente Account AWS a entrare a far parte della tua organizzazione](#).

3. Assicurati che tutti gli account membro siano associati all'account che desideri designare come unico account amministratore delegato GuardDuty . Disassocia qualsiasi account membro che è ancora associato agli account amministratore preesistenti.

I seguenti passaggi sono utili per disassociare gli account membri dall'account amministratore preesistente:

- a. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
 - b. Per accedere, utilizza le credenziali dell'account amministratore preesistente.
 - c. Dal riquadro di navigazione, selezionare Accounts (Account).
 - d. Nella pagina Account, seleziona uno o più account che desideri disassociare dall'account amministratore.
 - e. Scegli Operazioni, quindi Disassocia account.
 - f. Scegli Conferma per completare il passaggio.
4. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

Per accedere, utilizza le credenziali dell'account di gestione.

5. Nel pannello di navigazione scegli Impostazioni. Nella pagina Impostazioni, designa l'account GuardDuty amministratore delegato per l'organizzazione.
6. Accedere all'account amministratore delegato designato. GuardDuty
7. Aggiungi membri dall'organizzazione. Per ulteriori informazioni, consulta [Gestione GuardDuty degli account con AWS Organizations](#).

API/CLI

1. Tutti gli account che desideri gestire GuardDuty devono far parte della tua organizzazione. Per informazioni sull'aggiunta di un account alla tua organizzazione, vedi [Invitare un utente Account AWS a entrare a far parte della tua organizzazione](#).

2. Assicurati che tutti gli account membro siano associati all'account che desideri designare come unico account amministratore delegato GuardDuty .
 - a. Esegui [DisassociateMembers](#) per dissociare qualsiasi account membro ancora associato agli account amministratore preesistenti.
 - b. In alternativa, puoi utilizzare AWS Command Line Interface per eseguire il comando seguente e sostituirlo **777777777777** con l'ID del rilevatore dell'account amministratore preesistente da cui desideri dissociare l'account membro. Sostituiscilo **666666666666** con l' Account AWS ID dell'account membro da cui desideri dissociare.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
```

3. Esegui [EnableOrganizationAdminAccount](#) per delegare un Account AWS account come amministratore delegato. GuardDuty

In alternativa, puoi usare AWS Command Line Interface per eseguire il seguente comando per delegare un account amministratore delegato GuardDuty :

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Aggiungi membri dall'organizzazione. Per ulteriori informazioni, consulta [Create or add member member accounts using API](#).

Important

Per massimizzare l'efficacia di un servizio regionale GuardDuty, ti consigliamo di designare il tuo account GuardDuty amministratore delegato e aggiungere tutti gli account membro in ogni regione.

GuardDuty considerazioni sull'esportazione dei dettagli dell'account membro in formato CSV

In qualità di account GuardDuty amministratore, puoi esportare i dettagli dell'account membro in formato CSV. Questi dettagli includono l'ID dell'account membro, il nome, il tipo (aggiunto tramite

AWS Organizations o tramite invito), lo stato di configurazione GuardDuty e i piani di protezione dedicati.

L'opzione Esporta CSV viene visualizzata nella pagina GuardDuty Account in base al modo in cui gestisci gli account di più membri. Utilizzando l'opzione Esporta CSV, puoi identificare per quali account membro è abilitato un piano di protezione specifico.

L'elenco seguente fornisce i criteri per stabilire se il file Esporta CSV sarà disponibile o meno nella pagina GuardDuty Account:

- Lo utilizzi solo AWS Organizations per gestire più account membro e il numero totale di account membro nella tua GuardDuty organizzazione è fino a 5.000.
- Utilizzi entrambi i metodi AWS Organizations e il metodo degli inviti e il numero totale di account membri nella tua GuardDuty organizzazione è fino a 5.000.

In questo scenario, il file CSV esportato includerà se un account membro è stato aggiunto tramite AWS Organizations o utilizzando il metodo basato sugli inviti.

- Quando utilizzi solo il metodo basato su invito per gestire più account membri, non è disponibile l'opzione Esporta CSV.

GuardDuty tipi di ricerca

Un risultato è una notifica che viene GuardDuty generata quando rileva un'indicazione di un'attività sospetta o dannosa all'interno dell'utente. Account AWS GuardDuty genera un risultato in un account che è stato abilitato. GuardDuty

Per informazioni sulle modifiche importanti ai tipi di GuardDuty risultati, inclusi i tipi di risultati appena aggiunti o ritirati, vedere [Cronologia dei documenti per Amazon GuardDuty](#).

Per informazioni sui tipi di esiti che sono stati ritirati, consulta [Tipi di esiti ritirati](#).

GuardDuty Tipi di ricerca EC2

Gli esiti seguenti sono specifici per le risorse Amazon EC2 e hanno sempre un Tipo risorsa di Instance. La gravità e i dettagli degli esiti variano in base al ruolo risorsa, che indica se la risorsa EC2 è stata la destinazione di attività sospette o l'attore che le ha eseguite.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni sulle origini dati e sui modelli, consulta [GuardDuty fonti di dati fondamentali](#).

Note

- I dettagli dell'istanza di ricerca EC2 potrebbero mancare se l'istanza era già stata terminata o se la chiamata API sottostante proveniva da un'istanza EC2 in un'altra regione.
- I risultati di EC2 che utilizzano i log di flusso VPC come fonte di dati non supportano il traffico. IPv6

Per tutti gli esiti EC2, ti consigliamo di esaminare la risorsa in questione per determinare se si comporta nel modo previsto. Se l'attività è autorizzata, puoi utilizzare le regole di eliminazione o gli elenchi di indirizzi IP affidabili per prevenire notifiche false positive per quella risorsa. Se l'attività non è prevista, la best practice di sicurezza consiste nel presupporre che l'istanza sia stata compromessa e intraprendere le azioni dettagliate in [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Argomenti

- [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

Un'istanza EC2 esegue una query su un IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza elencata all'interno del tuo ambiente AWS esegue una query su un IP associato a un server di comando e controllo (C&C) noto. L'istanza elencata potrebbe essere compromessa. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet che può includere server PCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche emettere comandi per avviare un attacco Denial of Service (S) distribuito. DDo

Note

Se l'IP su cui viene eseguita una query è correlato a log4j, determinati campi dell'esito associato includeranno i valori seguenti:

- Servizio. Informazioni aggiuntive. threatListName = Amazon
- service.additionalInfo.threatName = Log4j Related

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/C&CActivity.B!DNS

Un'istanza EC2 esegue una query su un nome di dominio associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio associato a un server di comando e controllo (C&C) noto. L'istanza elencata potrebbe essere compromessa. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è un insieme di dispositivi connessi a Internet che può includere server PCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche emettere comandi per avviare un attacco Denial of Service (S) distribuito. DDo

Note

Se il nome di dominio su cui è stata eseguita la query è relativo a log4j, i campi dell'esito associato includeranno i valori seguenti:

- Servizio. Informazioni aggiuntive. threatListName = Amazon
- service.additionalInfo.threatName = Log4j Related

 Note

Per verificare come GuardDuty genera questo tipo di risultato, puoi effettuare una richiesta DNS dalla tua istanza (utilizzando `dig` per Linux o `nslookup` per Windows) su un dominio `guarddutyactivityb.com` di test.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/DenialOfService.Dns

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo DNS.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico DNS in uscita. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo DNS.

 Note

Questo esito rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/DenialOfService.Tcp

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo TCP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico TCP in uscita. Ciò può indicare che l'istanza è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo TCP.

Note

Questo esito rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/DenialOfService.Udp

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo UDP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico UDP in uscita. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo UDP.

 Note

Questo esito rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo UDP sulla porta TCP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico UDP in uscita indirizzato a una porta utilizzata di solito per le comunicazioni TCP. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo UDP su una porta TCP.

 Note

Questo esito rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/DenialOfService.UnusualProtocol

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando un protocollo insolito.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS genera un grande volume di traffico in uscita da un tipo di protocollo insolito che normalmente non è utilizzato dalle istanze EC2, ad esempio, l'Internet Group Management Protocol. Ciò può indicare che l'istanza è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando un protocollo insolito. Questo esito rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/Spambot

Un'istanza EC2 presenta un comportamento insolito in quanto comunica con un host remoto sulla porta 25.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS comunica con un host remoto sulla porta 25. Questo comportamento è inusuale in quanto l'istanza EC2 non ha mai comunicato sulla porta 25 in precedenza. La porta 25 è tradizionalmente utilizzata dai server di posta per le comunicazioni SMTP. Questo esito indica che l'istanza EC2 potrebbe essere compromessa per l'uso nell'invio di spam.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Behavior:EC2/NetworkPortUnusual

Un'istanza EC2 sta comunicando con un host remoto su una porta server inusuale.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. Questa istanza EC2 non ha mai comunicato su questa porta remota in precedenza.

Note

Se l'istanza EC2 ha comunicato sulla porta 389 o sulla porta 1389, la gravità dell'esito associata verrà modificata in "alta" e i campi dell'esito includeranno il valore seguente:

- `service.additionalInfo.context = Possible log4j callback`

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Behavior:EC2/TrafficVolumeUnusual

Un'istanza EC2 sta generando un volume di traffico di rete insolitamente elevato verso un host remoto.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 non ha mai inviato una tale quantità di traffico a questo host remoto in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

CryptoCurrency:EC2/BitcoinTool.B

Un'istanza EC2 sta eseguendo una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue una query su un indirizzo IP associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di CryptoCurrency:EC2/BitcoinTool.B. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere [Regole di soppressione in GuardDuty](#).

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

CryptoCurrency:EC2/BitcoinTool.B!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue una query su un nome di dominio associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere [Regole di soppressione in GuardDuty](#).

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

DefenseEvasion:EC2/UnusualDNSResolver

Un'istanza Amazon EC2 comunica con un resolver DNS pubblico insolito.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza Amazon EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dal comportamento di base. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni con questo resolver DNS pubblico. Il campo Unusual nel pannello dei dettagli di ricerca della GuardDuty console può fornire informazioni sul resolver DNS richiesto.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

DefenseEvasion:EC2/UnusualDoHActivity

Un'istanza Amazon EC2 esegue una comunicazione DNS su HTTPS (DoH) insolita.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni DNS su HTTPS (DoH) con questo server DoH pubblico. Il campo Insolito nei dettagli degli esiti può fornire informazioni sul server DoH su cui è stata effettuata la query.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

DefenseEvasion:EC2/UnusualDoTActivity

Un'istanza Amazon EC2 esegue una comunicazione DNS su TLS (DoT) insolita.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni DNS su TLS (DoT) con questo server DoT pubblico. Il campo Insolito nel pannello dei dettagli dell'esito può fornire informazioni sul server DoT su cui è stata effettuata la query.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/AbusedDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione associato a domini noti in abuso.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP noti in abuso. Esempi di domini in abuso sono i nomi di dominio di primo livello (TLD) e i nomi di dominio di secondo livello (2LD) che offrono registrazioni gratuite di sottodomini e provider DNS dinamici. Gli autori delle minacce tendono a utilizzare questi servizi per registrare domini gratuitamente o a basso costo. I domini a bassa reputazione di questa categoria possono anche essere domini scaduti che vengono sostituiti con l'indirizzo IP di parcheggio di un registrar e quindi potrebbero non essere più attivi. Un IP di parcheggio è il luogo in cui un registrar indirizza il traffico verso domini che non sono stati collegati ad alcun servizio. L'istanza Amazon EC2 elencata potrebbe essere compromessa poiché gli autori delle minacce utilizzano comunemente questi registrar o servizi per la distribuzione di malware e C&C.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/BitcoinDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di Impact:EC2/BitcoinDomainRequest.Reputation. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere [Regole di soppressione in GuardDuty](#).

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/MaliciousDomainRequest.Reputation

Un'istanza EC2 esegue una query su un dominio a bassa reputazione associato a domini dannosi noti.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP dannosi noti. Ad esempio, i domini possono essere associati a un indirizzo IP sinkhole noto. I domini sinkhole sono domini che sono stati precedentemente controllati da un autore di minacce e se vengono inoltrate richieste a questi domini può significare che l'istanza è compromessa. Questi domini possono anche essere correlati a campagne dannose note o algoritmi di generazione di domini.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/MaliciousDomainRequest.Custom

Un'istanza EC2 sta interrogando un dominio su un elenco di entità minacciose personalizzato.

Gravità predefinita: media

- Origine dati: log DNS

Questo risultato ti informa che l'istanza Amazon EC2 elencata nel AWS tuo ambiente sta interrogando un nome di dominio incluso nell'elenco delle entità minacciose che hai caricato e attivato. In GuardDuty, un elenco di entità minacciose è composto da nomi di dominio e indirizzi IP dannosi noti. GuardDuty genera risultati in base all'attività associata all'elenco delle entità minacciose caricato. È possibile visualizzare il nome dell'elenco delle entità minacciose nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/PortSweep

Su un gran numero di indirizzi IP è in corso il probing di una porta da parte di un'istanza EC2.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo risultato indica che l'istanza EC2 elencata nel tuo AWS ambiente sta sondando una porta su un gran numero di indirizzi IP instradabili pubblicamente. Questo tipo di attività viene in genere

utilizzato per trovare host vulnerabili da sfruttare. Nel pannello dei dettagli di ricerca GuardDuty della console, viene visualizzato solo l'indirizzo IP remoto più recente

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/SuspiciousDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione di natura sospetta a causa della sua età o della scarsa popolarità.

Gravità predefinita: bassa

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata nel tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione sospettato di essere dannoso. Abbiamo notato che le caratteristiche di questo dominio sono coerenti con i domini dannosi osservati in precedenza, ma il nostro modello di reputazione non è stato in grado di collegarlo in modo definitivo a una minaccia nota. Questi domini vengono in genere osservati per la prima volta o ricevono una quantità di traffico ridotta.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Impact:EC2/WinRMBruteForce

Un'istanza EC2 esegue un attacco di forza bruta di Windows Remote Management in uscita.

Gravità predefinita: bassa*

 Note

La gravità di questo esito è bassa se l'istanza EC2 era la destinazione di un attacco di forza bruta. La gravità di questo esito è alta se l'istanza EC2 è l'attore viene utilizzato per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue un attacco di forza bruta di Windows Remote Management (WinRM) volto a ottenere l'accesso al servizio Windows Remote Management su sistemi basati su Windows.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Recon:EC2/PortProbeEMRUnprotectedPort

Una porta non protetta EMR di un'istanza EC2 è sottoposta a probing da parte di un host dannoso noto.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo risultato indica che una porta sensibile relativa all'EMR sull'istanza EC2 elencata che fa parte di un cluster nel AWS tuo ambiente non è bloccata da un gruppo di sicurezza, da una lista di controllo degli accessi (ACL) o da un firewall on-host come Linux. IPTables Questo risultato indica inoltre che scanner noti su Internet stanno sondando attivamente questa porta. Le porte che possono attivare questo esito, ad esempio la porta 8088 (porta dell'interfaccia utente Web YARN), potrebbero potenzialmente essere utilizzate per l'esecuzione di codice in modalità remota.

Raccomandazioni per la correzione:

Ti consigliamo di bloccare l'accesso aperto alle porte su cluster da Internet e limitare l'accesso solo a indirizzi IP specifici che richiedono l'accesso a queste porte. Per ulteriori informazioni, consultare [Gruppi di sicurezza per cluster EMR](#).

Recon:EC2/PortProbeUnprotectedPort

Una porta non protetta di un'istanza EC2 è sottoposta a probing da parte di un host dannoso noto.

Gravità predefinita: bassa*

Note

La gravità predefinita di questi esiti è bassa. Tuttavia, se la porta che viene esaminata viene utilizzata da Elasticsearch (9200 o 9300), la gravità del risultato è elevata.

- Origine dati: log di flusso VPC

Questo risultato indica che una porta sull'istanza EC2 elencata nel tuo AWS ambiente non è bloccata da un gruppo di sicurezza, da una lista di controllo degli accessi (ACL) o da un firewall on-host come Linux IPTables, e che scanner noti su Internet la stanno esaminando attivamente.

Se la porta non protetta identificata è 22 o 3389 e si utilizzano queste porte per connettersi all'istanza, è comunque possibile limitare l'esposizione consentendo l'accesso a queste porte solo agli indirizzi IP dello spazio degli indirizzi IP della rete aziendale. Per limitare l'accesso alla porta 22 su Linux, consulta [Authorizing Inbound Traffic for Your Linux Instance](#). Per limitare l'accesso alla porta 3389 su Windows, consulta [Authorizing Inbound Traffic for Your Windows Instances](#).

GuardDuty non genera questo risultato per le porte 443 e 80.

Raccomandazioni per la correzione:

Tuttavia, ci possono essere casi in cui le istanze sono intenzionalmente esposte, ad esempio se ospitano server web. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di Recon:EC2/PortProbeUnprotectedPort. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da host bastione. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta [Regole di soppressione in GuardDuty](#).

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Recon:EC2/Portscan

Un'istanza EC2 sta eseguendo la scansione delle porte in uscita verso un host remoto.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS è coinvolta in un possibile attacco port scan in quanto sta effettuando più tentativi di connessione a diverse porte in un breve periodo di tempo. Lo scopo di un attacco port scan è di individuare le porte aperte per determinare quali servizi sono in esecuzione sulla macchina e per identificarne il sistema operativo.

Raccomandazioni per la correzione:

Questo esito può essere un falso positivo se nel tuo ambiente vengono implementate applicazioni di valutazione della vulnerabilità su istanze EC2. Queste applicazioni, infatti, eseguono scansioni delle porte per avvisarti in caso di porte aperte configurate in modo errato. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di Recon:EC2/Portscan. Il secondo criterio di filtro dovrebbe corrispondere all'istanza o alle istanze che ospitano questi strumenti di valutazione della vulnerabilità. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda dei criteri identificabili con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta [Regole di soppressione in GuardDuty](#).

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/BlackholeTraffic

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo risultato indica che l'istanza EC2 elencata nel tuo AWS ambiente potrebbe essere compromessa perché sta tentando di comunicare con l'indirizzo IP di un buco nero (o sink hole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/BlackholeTraffic!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio che è reindirizzato a un indirizzo IP di un buco nero.

Gravità predefinita: media

- Origine dati: log DNS

Questo risultato indica che l'istanza EC2 elencata nel tuo AWS ambiente potrebbe essere compromessa perché sta interrogando un nome di dominio che viene reindirizzato a un indirizzo IP di un buco nero. I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/DGADomainRequest.B

Un'istanza EC2 sta eseguendo una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS tenta di eseguire una query su domini DGA. L'istanza EC2 potrebbe essere compromessa.

DGAs vengono utilizzati per generare periodicamente un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

Note

L'esito è basato sull'analisi dei nomi di dominio tramite un'euristica avanzata e può quindi identificare nuovi domini DGA che non sono presenti nei feed di intelligence sulle minacce.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/DGADomainRequest.C!DNS

Un'istanza EC2 sta eseguendo una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS tenta di eseguire una query su domini DGA. L'istanza EC2 potrebbe essere compromessa.

DGAs vengono utilizzati per generare periodicamente un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I

server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

Note

Questa scoperta si basa su domini DGA noti provenienti dai feed di intelligence sulle minacce. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/DNSDataExfiltration

Un'istanza EC2 sta eseguendo l'esfiltrazione di dati tramite query DNS.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue un malware che utilizza query DNS per trasferire dati in uscita. Questo tipo di trasferimento di dati è indicativo di un'istanza compromessa e potrebbe comportare l'esfiltrazione di dati. Di solito, il traffico DNS non è bloccato dai firewall. Ad esempio, il malware in un'istanza EC2 compromessa può codificare i dati (ad esempio i numeri di carte di credito) in una query DNS e inviarli a un server DNS remoto controllato da un utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/DriveBySourceTraffic!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio di un host remoto che è l'origine nota di attacchi di download drive-by.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS potrebbe essere compromessa in quanto esegue una query su un nome di dominio di un host remoto che è un'origine nota di attacchi di download drive-by. Si tratta di download di software non voluti da Internet che possono attivare l'installazione automatica di virus, spyware o malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/DropPoint

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo risultato indica che un'istanza EC2 nel tuo AWS ambiente sta tentando di comunicare con un indirizzo IP di un host remoto noto per contenere credenziali e altri dati rubati catturati dal malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/DropPoint!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Origine dati: log DNS

Questo risultato indica che un'istanza EC2 nel tuo AWS ambiente sta interrogando un nome di dominio di un host remoto noto per contenere credenziali e altri dati rubati catturati dal malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Trojan:EC2/PhishingDomainRequest!DNS

Un'istanza EC2 sta eseguendo una query su domini implicati in attacchi di phishing. L'istanza EC2 potrebbe essere compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che nel tuo ambiente AWS è presente un'istanza EC2 che tenta di eseguire una query su un dominio implicato in attacchi di phishing. I domini di phishing sono configurati da individui che fingono di essere un'istituzione legittima allo scopo di indurre gli utenti a fornire dati sensibili come informazioni personali, coordinate bancarie, informazioni di carte di credito e password. L'istanza EC2 potrebbe tentare di recuperare dati sensibili archiviati su un sito Web di phishing oppure di configurare un sito Web di phishing. L'istanza EC2 potrebbe essere compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Un'istanza EC2 stabilisce connessioni a un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente sta comunicando con un indirizzo IP incluso in un elenco di minacce che hai caricato. In GuardDuty, un elenco di minacce è costituito da indirizzi IP dannosi noti. GuardDuty genera i risultati in base agli elenchi di minacce caricati. L'elenco delle minacce utilizzato per generare questo esito verrà elencato nei dettagli dell'esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

UnauthorizedAccess:EC2/MetadataDNSRebind

Un'istanza EC2 esegue ricerche DNS che vengono risolte nel servizio di metadati dell'istanza.

Gravità predefinita: alta

- Origine dati: log DNS

Questo risultato ti informa che un'istanza EC2 nel tuo AWS ambiente sta interrogando un dominio che si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). Una query DNS di questo tipo può indicare che l'istanza è la destinazione di una tecnica di rebinding DNS. Questa tecnica può essere utilizzata per ottenere metadati da un'istanza EC2, incluse le credenziali IAM a essa associate.

Il rebinding DNS implica l'inganno di un'applicazione in esecuzione sull'istanza EC2 per caricare i dati restituiti da un URL, dove il nome di dominio nell'URL si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). In questo modo l'applicazione accede ai metadati EC2 e, possibilmente, li rende disponibili all'utente malintenzionato.

Puoi accedere ai metadati EC2 utilizzando il rebinding DNS solo se l'istanza EC2 esegue un'applicazione vulnerabile che consente l'iniezione di URL oppure se qualcuno accede all'URL in un browser Web in esecuzione sull'istanza EC2.

Raccomandazioni per la correzione:

In risposta a questo esito, devi valutare se è presente un'applicazione vulnerabile in esecuzione sull'istanza EC2 o se qualcuno ha utilizzato un browser per accedere al dominio identificato nell'esito. Se la causa principale è un'applicazione vulnerabile, è necessario correggere la vulnerabilità. Se qualcuno ha navigato nel dominio identificato, è necessario bloccare il dominio o impedire agli utenti di accedervi. Se ritieni che l'esito sia correlato a uno dei due casi precedenti, [revoca la sessione associata all'istanza EC2](#).

Alcuni AWS clienti associano intenzionalmente l'indirizzo IP dei metadati a un nome di dominio sui propri server DNS autoritativi. Se questo è il caso del tuo ambiente, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Il secondo criterio di filtro deve essere il dominio di richiesta DNS e il valore deve corrispondere al dominio mappato all'indirizzo IP dei metadati (169.254.169.254). Per ulteriori informazioni sulla creazione di regole di soppressione, vedere [Regole di soppressione in GuardDuty](#).

UnauthorizedAccess:EC2/RDPBruteForce

Un'istanza EC2 è stata implicata in attacchi forza bruta RDP.

Gravità predefinita: bassa*

Note

La gravità di questo esito è bassa se l'istanza EC2 era la destinazione di un attacco di forza bruta. La gravità di questo esito è alta se l'istanza EC2 è l'attore viene utilizzato per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente è stata coinvolta in un attacco di forza bruta volto a ottenere le password per i servizi RDP su sistemi basati su Windows. Ciò può indicare un accesso non autorizzato alle risorse AWS .

Raccomandazioni per la correzione:

Se il Ruolo risorsa dell'istanza è ACTOR, significa che l'istanza è stata utilizzata per eseguire gli attacchi di forza bruta RDP. A meno che questa istanza non abbia un motivo legittimo per contattare l'indirizzo IP elencato come Target, ti consigliamo di presumere che l'istanza sia stata compromessa e di intraprendere le azioni elencate in [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Se il Resource Role dell'istanza è impostato su Resource RoleTARGET, questo problema può essere risolto rendendo sicura la porta RDP solo tramite Security Groups o firewall. IPs ACLs Per ulteriori informazioni, consulta [Suggerimenti per la protezione delle istanze EC2 \(Linux\)](#).

UnauthorizedAccess:EC2/SSHBruteForce

Un'istanza EC2 è stata implicata in attacchi forza bruta SSH.

Gravità predefinita: bassa*

Note

La gravità di questo esito è bassa se un attacco di forza bruta è rivolto a una delle istanze EC2. La gravità di questo esito è alta se l'istanza EC2 viene utilizzata per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente è stata coinvolta in un attacco di forza bruta volto a ottenere le password per i servizi SSH su sistemi basati su Linux. Ciò può indicare un accesso non autorizzato alle risorse AWS .

Note

Questo risultato viene generato solo dal monitoraggio del traffico di sulla porta 22. Se i servizi SSH sono configurati per utilizzare altre porte, questo esito non viene generato.

Raccomandazioni per la correzione:

Se l'obiettivo del tentativo di forza bruta è un host bastion, ciò potrebbe rappresentare il comportamento previsto per l'ambiente in uso. AWS In questo caso, si consiglia di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `UnauthorizedAccess:EC2/SSHBruteForce`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da host bastione. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta [Regole di soppressione in GuardDuty](#).

Se questa attività non è prevista per l'ambiente in uso e lo è il ruolo di risorsa dell'istanzaTARGET, è possibile porre rimedio a questo problema assicurando che la porta SSH sia affidabile solo IPs tramite gruppi di sicurezza o firewall. ACLs Per ulteriori informazioni, consulta [Suggerimenti per la protezione delle istanze EC2 \(Linux\)](#).

Se il Ruolo risorsa dell'istanza è ACTOR, questo indica che l'istanza è stata utilizzata per eseguire gli attacchi di forza bruta SSH. A meno che questa istanza non abbia un motivo legittimo per contattare l'indirizzo IP elencato come Target, ti consigliamo di presumere che l'istanza sia stata compromessa e di intraprendere le azioni elencate in [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

UnauthorizedAccess:EC2/TorClient

L'istanza EC2 sta stabilendo connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che l'istanza EC2 è stata compromessa e funge da client su una rete Tor. Questa scoperta potrebbe indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

UnauthorizedAccess:EC2/TorRelay

L'istanza EC2 sta stabilendo connessioni a una rete Tor come relay Tor.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

GuardDuty Tipi di ricerca IAM

Gli esiti seguenti sono specifici per le entità IAM e le chiavi di accesso e avranno sempre un Tipo risorsa di AccessKey. La gravità e i dettagli degli esiti variano in base al tipo di esito.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni, consulta [GuardDuty fonti di dati fondamentali](#).

Per tutti gli esiti relativi a IAM, ti consigliamo di esaminare l'entità in questione e assicurarti che le relative autorizzazioni seguano la best practice del privilegio minimo. Se l'attività non è prevista, le credenziali potrebbero essere compromesse. Per informazioni su come correggere gli esiti, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Argomenti

- [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.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)

CredentialAccess:IAMUser/AnomalousBehavior

Un'API utilizzata per accedere a un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account.

Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica [identità utente](#). L'API osservata è comunemente associata alla fase di accesso alle credenziali di un attacco, quando un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il tuo ambiente. APIs In questa categoria ci sono GetPasswordDataGetSecretValue, BatchGetSecretValue, e GenerateDbAuthToken.

Questa richiesta API è stata identificata come anomala dal modello ML (Anomaly GuardDuty Detection Machine Learning) di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

CredentialAccess:IAMUser/CompromisedCredentials

Una chiave di accesso IAM è stata identificata come potenzialmente compromessa dalla threat intelligence di Amazon.

Gravità predefinita: alta

- Funzionalità: inclusa con Foundational Data Source Protection

Descrizione completa:

Questa scoperta ti informa che una chiave di accesso IAM associata al tuo AWS account è stata identificata come potenzialmente compromessa dalla threat intelligence di Amazon. La credenziale compromessa è stata quindi utilizzata per richiamare le operazioni API nel tuo ambiente. AWS L'elenco delle chiamate API effettuate utilizzando la credenziale compromessa, insieme al conteggio e ai timestamp di ogni chiamata, alla chiave di accesso coinvolta e all'indirizzo IP di origine sono inclusi nei dettagli del risultato.

La compromissione delle credenziali in questa scoperta è stata identificata dalla threat intelligence di Amazon. AWS monitora le credenziali potenzialmente compromesse attraverso i modelli di utilizzo e genera questo risultato quando si osserva che tale credenziale viene utilizzata.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

DefenseEvasion:IAMUser/AnomalousBehavior

Un'API utilizzata per eludere le misure difensive è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è comunemente associata a tattiche di evasione difensiva in cui un avversario cerca di nascondere le proprie tracce ed evitare di essere scoperto. APIs in questa categoria si trovano in genere operazioni di eliminazione, disabilitazione o interruzione, come, o. DeleteFlowLogs DisableAlarmActions StopLogging

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

DefenseEvasion:IAMUser/BedrockLoggingDisabled

La registrazione per Amazon Bedrock è stata disattivata.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che la registrazione è stata disattivata per le invocazioni del modello Bedrock nel tuo account. Questo può essere il tentativo di un utente malintenzionato di nascondere attività dannose come l'esfiltrazione di dati o l'abuso di modelli di IA. La disabilitazione della registrazione rimuove la visibilità dei dati inviati ai modelli e del modo in cui i modelli vengono utilizzati.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Discovery:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per scovare le risorse è stata richiamata in modo anomalo.

Gravità predefinita: bassa

- Fonte dei dati: evento CloudTrail di gestione

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è generalmente associata alla fase di scoperta di un attacco, quando un avversario raccoglie informazioni per determinare se l'AWS ambiente è suscettibile a un attacco più ampio. APIs in questa categoria rientrano in genere operazioni di recupero, descrizione o elenco, ad esempio, `DescribeInstances` o `GetRolePolicy` `ListAccessKeys`.

Questa richiesta API è stata identificata come anomala dal modello ML (GuardDutyAnomaly Detection Machine Learning). Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata

effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Exfiltration:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per raccogliere dati da un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è comunemente associata a tattiche di esfiltrazione in cui un avversario cerca di raccogliere dati dalla rete utilizzando pacchetti e crittografia per evitare il rilevamento. APIs per questo tipo di risultato si tratta solo di operazioni di gestione (piano di controllo) e sono in genere correlate a S3, alle istantanee e ai database, come,, o. PutBucketReplication CreateSnapshot RestoreDBInstanceFromDBSnapshot

Questa richiesta API è stata identificata come anomala dal modello di machine learning (ML) per GuardDuty il rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Impact:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per manomettere dati o processi in un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è comunemente associata a tattiche di impatto in cui un avversario cerca di interrompere le operazioni e manipolare, interrompere o distruggere i dati dell'account. APIs per questo tipo di risultato si utilizzano in genere operazioni di eliminazione, aggiornamento o invio, come, o. DeleteSecurityGroup UpdateUser PutBucketPolicy

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

InitialAccess:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per ottenere l'accesso non autorizzato a un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è generalmente associata alla fase di accesso iniziale di un attacco, quando un avversario tenta di stabilire l'accesso all'ambiente. APIs in questa categoria rientrano in genere operazioni get token o di sessione, come, `StartSession` o `GetAuthorizationToken`.

Questa richiesta API è stata identificata come anomala dal modello ML (GuardDutyAnomaly Detection Machine Learning). Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

PenTest:IAMUser/KaliLinux

Un'API è stata richiamata da una macchina Kali Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che una macchina che esegue Kali Linux sta effettuando chiamate API utilizzando credenziali che appartengono all' AWS account elencato nel tuo ambiente. Kali Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

PenTest:IAMUser/ParrotLinux

Un'API è stata richiamata da una macchina Parrot Security Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta indica che una macchina che esegue Parrot Security Linux sta effettuando chiamate API utilizzando credenziali che appartengono all' AWS account elencato nell'ambiente in uso. Parrot Security Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato all'ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

PenTest:IAMUser/PentooLinux

Un'API è stata richiamata da una macchina Pentoo Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che una macchina che esegue Pentoo Linux sta effettuando chiamate API utilizzando credenziali che appartengono all' AWS account elencato nel tuo ambiente. Pentoo Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Persistence:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per mantenere l'accesso non autorizzato a un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso all'ambiente dell'utente e sta tentando di mantenere tale accesso. APIs in questa categoria si trovano in genere operazioni di creazione, importazione o modifica, come, o. CreateAccessKey ImportKeyPair ModifyInstanceAttribute

Questa richiesta API è stata identificata come anomala dal modello ML (GuardDutyAnomaly Detection Machine Learning). Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Policy:IAMUser/RootCredentialUsage

Un'API è stata richiamata utilizzando le credenziali di accesso di un utente root.

Gravità predefinita: bassa

- Fonte dati: eventi di CloudTrail gestione o eventi relativi ai CloudTrail dati per S3

Questo esito segnala che le credenziali di accesso dell'utente root dell' Account AWS elencato nel tuo ambiente vengono utilizzate per effettuare richieste ai servizi AWS . Si consiglia agli utenti di

non utilizzare mai le credenziali di accesso dell'utente root per accedere ai servizi. AWS È invece necessario accedere AWS ai servizi utilizzando le credenziali temporanee con privilegi minimi di (STS). AWS Security Token Service Nelle situazioni in cui AWS STS non è supportato, consigliamo di utilizzare le credenziali dell'utente IAM. Per ulteriori informazioni, consulta [Best Practice IAM](#).

Note

Se S3 Protection è abilitato per l'account, questo risultato può essere generato in risposta ai tentativi di eseguire operazioni sul piano dati S3 sulle risorse Amazon S3 utilizzando le credenziali di accesso dell'utente root di Account AWS. La chiamata API utilizzata verrà elencata nei dettagli dell'esito. Se S3 Protection non è abilitato, questo risultato può essere attivato solo dal registro eventi. APIs Per ulteriori informazioni su S3 Protection, consulta [Protezione S3](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Policy: IAMUser/ShortTermRootCredentialUsage

È stata invocata un'API utilizzando credenziali utente root limitate.

Gravità predefinita: bassa

- Fonte dati: eventi di AWS CloudTrail gestione o eventi AWS CloudTrail relativi ai dati per S3

Questa scoperta ti informa che le credenziali utente con restrizioni create per gli utenti elencati Account AWS nel tuo ambiente vengono utilizzate per effettuare richieste a Servizi AWS. Si consiglia di utilizzare le credenziali dell'utente root solo per quelle [attività che richiedono credenziali utente root](#).

Quando possibile, accedi Servizi AWS utilizzando i ruoli IAM con privilegi minimi con credenziali temporanee da (). AWS Security Token Service AWS STS Per gli scenari in cui non AWS STS è supportato, la best practice consiste nell'utilizzare le credenziali utente IAM. Per ulteriori informazioni, consulta le [best practice di sicurezza in IAM](#) e le [migliori pratiche per gli utenti root per te Account AWS](#) nella IAM User Guide.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

PrivilegeEscalation:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per ottenere autorizzazioni di alto livello per un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola API o una serie di richieste API correlate effettuate in prossimità da una singola [identità utente](#). L'API osservata è comunemente associata a tattiche di escalation dei privilegi in cui un avversario tenta di ottenere autorizzazioni di livello superiore per un ambiente. APIs in questa categoria si tratta in genere di operazioni che modificano le politiche, i ruoli e gli utenti di IAM, ad esempio, o. AssociateIamInstanceProfile AddUserToGroup PutUserPolicy

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei [dettagli sugli esiti](#) sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Recon:IAMUser/MaliciousIPCaller

Un'API è stata chiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che un'operazione API in grado di elencare o descrivere le risorse AWS di un account all'interno del tuo ambiente è stata richiamata da un indirizzo IP incluso in un elenco minacce. Un utente malintenzionato può utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali già in suo possesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Recon:IAMUser/MaliciousIPCaller.Custom

Un'API è stata chiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che un'operazione API in grado di elencare o descrivere le risorse AWS di un account all'interno del tuo ambiente è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato. L'elenco delle minacce utilizzato sarà elencato nei dettagli dell'esito. Un utente malintenzionato potrebbe utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali già in suo possesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Recon:IAMUser/TorIPCaller

Un'API è stata chiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che un'operazione API in grado di elencare o descrivere le risorse AWS di un account all'interno del tuo ambiente è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Un utente malintenzionato può usare Tor per mascherare la propria identità.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail la registrazione è stata disabilitata.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta indica che una CloudTrail traccia all'interno AWS dell'ambiente in uso è stata disattivata. Può trattarsi di un tentativo di un utente malintenzionato di disabilitare la registrazione per eliminare le tracce della sua attività accedendo nel contempo alle risorse AWS per scopi dannosi. Questo esito può essere generato dall'eliminazione o dall'aggiornamento riuscito di un trail, Questo risultato può essere innescato anche dall'eliminazione riuscita di un bucket S3 che memorizza i log di un trail associato a GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Stealth:IAMUser/PasswordPolicyChange

La policy delle password dell'account è stata indebolita.

Gravità predefinita: bassa*

 Note

La gravità di questo esito può essere bassa, media o alta a seconda della gravità delle modifiche apportate alla policy delle password.

- Fonte dei dati: eventi di gestione CloudTrail

La politica relativa alle password degli AWS account è stata indebolita nell'account elencato nell'AWS ambiente in uso. Ad esempio, è stata eliminata o aggiornata per richiedere un numero minore di caratteri, non richiedere simboli e numeri o per prolungare l'estensione del periodo di scadenza delle password. Questo risultato può essere causato anche dal tentativo di aggiornare o eliminare la politica relativa alle password AWS dell'account. La politica sulle password degli AWS account definisce le regole che regolano i tipi di password che possono essere impostati per gli utenti IAM. Un policy delle password indebolita consente la creazione di password facili da ricordare e potenzialmente più facili da indovinare, creando di fatto un rischio per la sicurezza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Molteplici connessioni riuscite alla console sono state osservate in tutto il mondo.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che molteplici connessioni riuscite alla console da parte dello stesso utente IAM sono state osservate simultaneamente in varie regioni geografiche. Questi modelli di localizzazione degli accessi anomali e rischiosi indicano un potenziale accesso non autorizzato alle risorse dell'utente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Credenziali create in modo esclusivo per un'istanza EC2 mediante un ruolo di avvio di istanze vengono utilizzate da un altro account all'interno di AWS.

Gravità predefinita: alta*

Note

La gravità predefinita di questi esiti è alta. Tuttavia, se l'API è stata richiamata da un account affiliato all' AWS ambiente in uso, la gravità è Media.

- Fonte dei dati: eventi di CloudTrail gestione o eventi CloudTrail relativi ai dati per S3

Questo risultato ti informa quando le credenziali dell'istanza Amazon EC2 vengono utilizzate per API richiamare da un indirizzo IP o da un endpoint Amazon VPC, di proprietà di un account AWS diverso da quello su cui è in esecuzione l'istanza Amazon EC2 associata. Il rilevamento degli endpoint VPC è disponibile solo per i servizi che supportano eventi di attività di rete per gli endpoint VPC. Per informazioni sui servizi che supportano gli eventi di attività di rete per gli endpoint VPC, consulta [Registrazione degli eventi di attività di rete](#) nella Guida per l'utente di AWS CloudTrail .

AWS non consiglia di ridistribuire le credenziali temporanee al di fuori dell'entità che le ha create (ad esempio, AWS applicazioni, Amazon EC2 o). AWS Lambda Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie istanze Amazon EC2 per rendere legittime le chiamate API. Se il `remoteAccountDetails.Affiliated` campo è, `True` l'API è stata richiamata da un account associato allo stesso account amministratore. Per escludere un potenziale attacco e verificare la legittimità dell'attività, contatta il Account AWS proprietario o il responsabile IAM a cui sono assegnate queste credenziali.

Note

Se GuardDuty rileva un'attività continua da un account remoto, il suo modello di machine learning (ML) la identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'account remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri account

remoti e rivaluterà gli account remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

Questo risultato viene generato quando le richieste AWS API vengono effettuate all'interno AWS tramite un'istanza Amazon EC2 esterna alla tua Account AWS, utilizzando le credenziali di sessione dell'istanza Amazon EC2. Potrebbe essere consuetudine, ad esempio per l'architettura Transit Gateway in una configurazione [hub and spoke](#), instradare il traffico attraverso un singolo VPC di uscita dell'hub con endpoint di servizio. AWS Se è previsto questo comportamento, ti GuardDuty consiglia di utilizzare [Regole di eliminazione](#) e creare una regola con criteri a due filtri. Il primo criterio è il tipo di esito, che, in questo caso, è UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Il secondo criterio di filtro è l'ID account remoto dei dettagli dell'account remoto.

In risposta a questo esito, puoi utilizzare il seguente flusso di lavoro per determinare una linea d'azione:

1. Identifica l'account remoto coinvolto tramite il campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Determina direttamente sul campo se quell'account è affiliato al tuo GuardDuty ambiente. `service.action.awsApiCallAction.remoteAccountDetails.affiliated`
3. Se l'account è affiliato, contatta il proprietario dell'account remoto e il proprietario delle credenziali dell'istanza Amazon EC2 per indagare.

Se l'account non è affiliato, il primo passo consiste nel valutare se quell'account è associato alla tua organizzazione ma non fa parte della configurazione dell'ambiente con GuardDuty più account o se GuardDuty non è ancora stato abilitato in questo account. In caso contrario, contatta il proprietario delle credenziali dell'istanza Amazon EC2 per determinare se esiste un caso d'uso per l'utilizzo di tali credenziali da parte di un account remoto.

4. Se il proprietario non riconosce l'account remoto, allora le credenziali potrebbero essere state compromesse da un autore di minacce che opera all'interno di AWS. È necessario adottare le misure consigliate in [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#), per proteggere il proprio ambiente.

Inoltre, puoi [inviare una segnalazione di abuso](#) al team AWS Trust and Safety per avviare un'indagine sull'account remoto. Quando invii la segnalazione a AWS Trust and Safety, includi i dettagli JSON completi del risultato.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Credenziali create in modo esclusivo per un'istanza EC2 mediante un ruolo di avvio di istanze vengono utilizzate da un indirizzo IP esterno.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail gestione o eventi CloudTrail relativi ai dati per S3

Questo risultato indica che un host esterno AWS ha tentato di eseguire operazioni AWS API utilizzando AWS credenziali temporanee create su un'istanza EC2 nel tuo ambiente. AWS L'istanza EC2 elencata potrebbe essere compromessa e le credenziali temporanee di questa istanza potrebbero essere state esfiltrate su un host remoto esterno a. AWS AWS non consiglia di ridistribuire le credenziali temporanee all'esterno dell'entità che le ha create (ad esempio, AWS applicazioni, EC2 o Lambda). Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie istanze EC2 per rendere legittime le chiamate API. Per escludere un potenziale attacco e verificare la legittimità dell'attività, verifica se nell'esito è previsto l'uso di credenziali di istanza provenienti dall'IP remoto.

Note

Se GuardDuty rileva un'attività continua da un host remoto, il relativo modello di machine learning (ML) la identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'host remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri host remoti e rivaluterà gli host remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

Questo esito viene generato quando la rete è configurata per instradare il traffico Internet in modo tale da uscire da un gateway on-premise anziché da un gateway Internet (IGW)

VPC. Configurazioni comuni, come l'utilizzo di [AWS Outposts](#) o delle connessioni VPN del VPC, possono instradare il traffico in questo modo. Se questo comportamento è previsto, ti consigliamo di utilizzare le regole di eliminazione e creare una regola composta da due criteri di filtro. Il primo criterio è tipo di esito, che dovrebbe essere `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'IPv4 indirizzo del chiamante API con l'indirizzo IP o l'intervallo CIDR del gateway Internet locale. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere [Regole di soppressione in GuardDuty](#).

Note

Se GuardDuty rileva un'attività continua proveniente da una fonte esterna, il suo modello di apprendimento automatico la identificherà come comportamento previsto e smetterà di generare questo risultato per l'attività proveniente da quella fonte. GuardDuty continuerà a generare risultati per nuovi comportamenti da altre fonti e rivaluterà le fonti apprese man mano che il comportamento cambia nel tempo.

Se questa attività non è prevista, le credenziali potrebbero essere compromesse, vedere [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Un'API è stata chiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che un'operazione API (ad esempio, un tentativo di avviare un'istanza EC2, creare un nuovo utente IAM o modificare i privilegi AWS) è stata richiamata da un indirizzo IP dannoso noto. Ciò può indicare un accesso non autorizzato alle AWS risorse all'interno dell'ambiente.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Un'API è stata chiamata da un indirizzo IP incluso in un elenco di minacce personalizzato.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta ti informa che un'operazione API (ad esempio, un tentativo di avviare un'istanza EC2, creare un nuovo utente IAM o modificare AWS i privilegi) è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. In GuardDuty, un elenco di minacce è composto da indirizzi IP dannosi noti. Ciò può indicare un accesso non autorizzato alle AWS risorse all'interno dell'ambiente.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS

Le credenziali create esclusivamente per una AWS Lambda risorsa vengono utilizzate da un indirizzo IP esterno a. AWS

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail gestione o eventi CloudTrail relativi ai dati per S3

Questo risultato indica che un host esterno a Internet AWS ha tentato di eseguire operazioni AWS API utilizzando AWS credenziali temporanee create su una AWS Lambda risorsa del tuo ambiente. AWS La risorsa Lambda elencata potrebbe essere compromessa e le credenziali temporanee di questa Lambda potrebbero essere state esfiltrate su un host remoto esterno a. AWS

AWS non consiglia di ridistribuire le credenziali temporanee al di fuori dell'entità che le ha create (ad esempio applicazioni AWS come Amazon Elastic Compute Cloud (Amazon EC2) o). AWS Lambda Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie risorse Lambda per rendere legittime le chiamate API. Per escludere un potenziale attacco e verificare la legittimità dell'attività, verifica se nell'esito è previsto l'uso di credenziali di istanza provenienti dall'IP remoto.

 Note

Se GuardDuty rileva un'attività continua da un host remoto, il modello di machine learning (ML) lo identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'host remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri host remoti e rivaluterà gli host remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

Questo esito viene generato quando la rete è configurata per instradare il traffico Internet in modo tale da uscire da un gateway on-premises anziché da un gateway Internet (IGW) VPC. Configurazioni comuni, come l'utilizzo di [AWS Outposts](#) o delle connessioni VPN del VPC, possono instradare il traffico in questo modo. Se si tratta di un comportamento previsto, ne GuardDuty consiglia l'utilizzo [Regole di eliminazione](#) per creare una regola con criteri a due filtri. Il primo criterio è tipo di esito, che dovrebbe essere `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'IPv4 indirizzo del chiamante API con l'indirizzo IP o l'intervallo CIDR per il gateway Internet locale.

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per informazioni sui passaggi per correggere questo tipo di risultato, vedere. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

UnauthorizedAccess:IAMUser/TorIPCaller

Un'API è stata chiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che un'operazione API (ad esempio, un tentativo di avviare un'istanza EC2, creare un nuovo utente IAM o modificare i privilegi AWS) è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

GuardDuty tipi di ricerca della sequenza di attacco

GuardDuty rileva una sequenza di attacco quando una sequenza specifica di più azioni si allinea a un'attività potenzialmente sospetta. Una sequenza di attacco include segnali come le attività e i risultati delle API. Quando GuardDuty osserva un gruppo di segnali in una sequenza specifica che indica una minaccia alla sicurezza in corso, in corso o recente, GuardDuty genera una rilevazione della sequenza di attacco. GuardDuty considera le singole attività delle API come [weak signals](#) se non si presentassero come una potenziale minaccia.

I rilevamenti delle sequenze di attacco si concentrano sulla potenziale compromissione dei dati di Amazon S3 (che possono far parte di un attacco ransomware più ampio), sulle credenziali AWS compromesse, sui cluster Amazon EKS, sui cluster Amazon ECS compromessi e sui gruppi di istanze Amazon EC2 compromessi. Le seguenti sezioni forniscono dettagli su ciascuna delle sequenze di attacco.

Argomenti

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:ECS/CompromisedCluster](#)
- [AttackSequence:EC2/CompromisedInstanceGroup](#)
- [AttackSequence:IAM/CompromisedCredentials](#)
- [AttackSequence:S3/CompromisedData](#)

AttackSequence:EKS/CompromisedCluster

Una sequenza di azioni sospette eseguite da un cluster Amazon EKS potenzialmente compromesso.

- Severità predefinita: critica
- Fonti di dati:
 - [Eventi del registro di controllo EKS](#)
 - [Monitoraggio del runtime per Amazon EKS](#)

- [Rilevamento di malware Amazon EKS per Amazon EC2](#)
- [AWS CloudTrail eventi relativi ai dati per S3](#)
- [AWS CloudTrail eventi di gestione](#)
- [Log di flusso VPC](#)
- [Registri delle query DNS di Route53 Resolver](#)

Questo risultato indica che è GuardDuty stata rilevata una sequenza di azioni sospette che indica un cluster Amazon EKS potenzialmente compromesso nel tuo ambiente. Nello stesso cluster Amazon EKS sono stati osservati diversi comportamenti di attacco sospetti e anomali, come processi dannosi o connessioni con endpoint dannosi.

GuardDuty utilizza i suoi algoritmi di correlazione proprietari per osservare e identificare la sequenza di azioni eseguite utilizzando la credenziale IAM. GuardDuty valuta i risultati dei piani di protezione e di altre fonti di segnale per identificare modelli di attacco comuni ed emergenti. GuardDuty utilizza diversi fattori per far emergere le minacce, come la reputazione IP, le sequenze API, la configurazione degli utenti e le risorse potenzialmente interessate.

Azioni correttive: se questo comportamento è imprevisto nel tuo ambiente, il cluster Amazon EKS potrebbe essere compromesso. Per una guida completa sulla riparazione, consulta e. [Correzione dei risultati della protezione EKS](#) [Riparazione degli esiti del monitoraggio del runtime](#)

Inoltre, poiché AWS le credenziali potrebbero essere state compromesse attraverso il cluster EKS, vedi. [Riparazione delle credenziali potenzialmente compromesse AWS](#) Per informazioni sulle procedure per correggere altre risorse che potrebbero essere state potenzialmente compromesse, consulta. [Correzione dei problemi di GuardDuty sicurezza rilevati](#)

AttackSequence:ECS/CompromisedCluster

Una sequenza di azioni sospette eseguite da un cluster Amazon ECS potenzialmente compromesso.

- Gravità predefinita: critica
- Fonti di dati:
 - [Monitoraggio del runtime per Amazon ECS Fargate](#)
 - [Monitoraggio del runtime per istanze EC2 in Amazon ECS](#)
 - [GuardDuty Protezione da malware per Amazon EC2](#)

Questo risultato indica che è GuardDuty stata rilevata una sequenza di segnali sospetti che indicano un cluster Amazon ECS potenzialmente compromesso nel tuo ambiente. Questi segnali possono includere processi dannosi, comunicazioni con endpoint dannosi o comportamenti di mining di criptovalute.

GuardDuty utilizza algoritmi di correlazione proprietari e molteplici fattori di rilevamento per identificare sequenze di azioni sospette all'interno dei cluster Amazon ECS. Attraverso l'analisi dei piani di protezione e di varie fonti di segnale, GuardDuty identifica i modelli di attacco comuni ed emergenti, garantendo un rilevamento estremamente sicuro di potenziali compromissioni.

Azioni correttive: se questo comportamento è imprevisto nel tuo ambiente, il tuo cluster Amazon ECS potrebbe essere compromesso. Per consigli sul contenimento delle minacce, consulta. [Riparazione di un cluster ECS potenzialmente compromesso](#) Tieni presente che il compromesso può estendersi a una o più attività ECS o carichi di lavoro dei container, che avrebbero potuto essere utilizzati per creare o modificare risorse. AWS Per una guida completa sulla riparazione che copre le risorse potenzialmente interessate, consulta. [Correzione dei problemi di GuardDuty sicurezza rilevati](#)

AttackSequence:EC2/CompromisedInstanceGroup

Una sequenza di azioni sospette che indica istanze Amazon EC2 potenzialmente compromesse.

- Gravità predefinita: critica
- Fonti di dati:
 - [Monitoraggio del runtime per Amazon EC2](#)
 - [Rilevamento di malware per Amazon EC2](#)
 - [Log di flusso VPC](#)
 - [Registri delle query DNS di Route53 Resolver](#)

Questo risultato indica che è GuardDuty stata rilevata una sequenza di azioni sospette che suggeriscono una potenziale compromissione in un gruppo di istanze Amazon EC2 nel tuo ambiente. I gruppi di istanze rappresentano in genere applicazioni gestite tramite infrastructure-as-code, che condividono configurazioni simili come il gruppo di scalabilità automatica, il ruolo del profilo dell'istanza IAM, lo AWS CloudFormation stack, il modello di lancio di Amazon EC2, l'AMI o l'ID VPC. GuardDuty ha osservato diversi comportamenti sospetti in una o più istanze, tra cui:

- Processi dannosi

- File dannosi
- Connessioni di rete sospette
- Attività di mining di criptovalute
- Utilizzo sospetto delle credenziali dell'istanza Amazon EC2

Metodo di rilevamento: GuardDuty utilizza algoritmi di correlazione proprietari per identificare sequenze di azioni sospette all'interno delle istanze Amazon EC2. Valutando i risultati dei piani di protezione e di varie fonti di segnale, GuardDuty identifica i modelli di attacco utilizzando molteplici fattori come la reputazione dell'IP e del dominio e i processi in esecuzione sospetti.

Azioni correttive: se questo comportamento è imprevisto nel tuo ambiente, le tue istanze Amazon EC2 potrebbero essere compromesse. Il compromesso potrebbe comportare:

- Processi multipli
- Credenziali di istanza che potrebbero essere state utilizzate per modificare le istanze di Amazon EC2 o altre risorse AWS

Per consigli sul contenimento delle minacce, consulta. [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#) Tieni presente che il compromesso può estendersi a una o più istanze Amazon EC2 e comportare processi o credenziali di istanza compromessi che avrebbero potuto essere utilizzati per creare o modificare istanze Amazon EC2 o altre risorse. AWS Per una guida completa sulla riparazione che copre le risorse potenzialmente interessate, consulta. [Correzione dei problemi di GuardDuty sicurezza rilevati](#)

AttackSequence:IAM/CompromisedCredentials

Una sequenza di richieste API che sono state richiamate utilizzando credenziali potenzialmente compromesse. AWS

- Gravità predefinita: Critica
- Fonte dei dati: [AWS CloudTrail eventi di gestione](#)

Questo risultato indica che è GuardDuty stata rilevata una sequenza di azioni sospette eseguite utilizzando AWS credenziali che hanno un impatto su una o più risorse dell'ambiente. Sono stati osservati più comportamenti di attacco sospetti e anomali con le stesse credenziali, con conseguente maggiore certezza che le credenziali vengano utilizzate in modo improprio.

GuardDuty utilizza i propri algoritmi di correlazione proprietari per osservare e identificare la sequenza di azioni eseguite utilizzando la credenziale IAM. GuardDuty valuta i risultati dei piani di protezione e di altre fonti di segnale per identificare modelli di attacco comuni ed emergenti. GuardDuty utilizza diversi fattori per far emergere le minacce, come la reputazione IP, le sequenze API, la configurazione degli utenti e le risorse potenzialmente interessate.

Azioni correttive: se questo comportamento è imprevisto nell'ambiente in uso, è possibile che le AWS credenziali siano state compromesse. Per le procedure da seguire per rimediare, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#). Le credenziali compromesse potrebbero essere state utilizzate per creare o modificare risorse aggiuntive, come bucket Amazon S3, funzioni o istanze Amazon EC2 AWS Lambda, nel tuo ambiente. Per informazioni su come correggere altre risorse che potrebbero essere state potenzialmente compromesse, consulta [Correzione dei problemi di GuardDuty sicurezza rilevati](#).

AttackSequence:S3/CompromisedData

È stata richiamata una sequenza di richieste API in un potenziale tentativo di esfiltrare o distruggere dati in Amazon S3.

- Gravità predefinita: critica
- Fonti di dati: [AWS CloudTrail eventi relativi ai dati per S3](#) e [AWS CloudTrail eventi di gestione](#)

Questo risultato indica che è GuardDuty stata rilevata una sequenza di azioni sospette indicative di una compromissione dei dati in uno o più bucket Amazon Simple Storage Service (Amazon S3), utilizzando credenziali potenzialmente compromesse. AWS Sono stati osservati diversi comportamenti di attacco sospetti e anomali (richieste API), con conseguente maggiore fiducia nell'uso improprio delle credenziali.

GuardDuty utilizza i suoi algoritmi di correlazione per osservare e identificare la sequenza di azioni eseguite utilizzando la credenziale IAM. GuardDuty quindi valuta i risultati dei piani di protezione e di altre fonti di segnale per identificare modelli di attacco comuni ed emergenti. GuardDuty utilizza diversi fattori per far emergere le minacce, come la reputazione IP, le sequenze API, la configurazione degli utenti e le risorse potenzialmente interessate.

Azioni correttive: se questa attività è imprevista nel tuo ambiente, AWS le tue credenziali o i dati di Amazon S3 potrebbero essere stati potenzialmente esfiltrati o distrutti. Per le procedure di correzione, consulta e. [Riparazione delle credenziali potenzialmente compromesse AWS](#) [Riparazione di un bucket S3 potenzialmente compromesso](#)

GuardDuty S3 Tipi di risultati di protezione

I seguenti risultati sono specifici per le risorse di Amazon S3 e avranno un tipo di risorsa **S3Bucket** se l'origine CloudTrail dati è data events per S3 o **AccessKey** se l'origine dati è CloudTrail un evento di gestione. La gravità e i dettagli dei risultati saranno diversi in base al tipo di ricerca e all'autorizzazione associata al bucket.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni sulle origini dati e sui modelli, consulta [GuardDuty fonti di dati fondamentali](#).

Important

I risultati con una fonte di dati sugli eventi di CloudTrail dati per S3 vengono generati solo se hai abilitato S3 Protection. Per impostazione predefinita, dopo il 31 luglio 2020, S3 Protection è abilitato quando un account viene abilitato GuardDuty per la prima volta o quando un account GuardDuty amministratore delegato viene abilitato GuardDuty in un account membro esistente. Tuttavia, quando un nuovo membro si unisce all' GuardDuty organizzazione, verranno applicate le preferenze di attivazione automatica dell'organizzazione. Per informazioni sull'attivazione automatica delle preferenze, consulta [Impostazione delle preferenze di attivazione automatica dell'organizzazione](#). Per informazioni su come abilitare S3 Protection, vedi [GuardDuty Protezione S3](#)

Per tutti i tipi di esiti S3Bucket, ti consigliamo di esaminare le autorizzazioni sul bucket in questione e le autorizzazioni di tutti gli utenti coinvolti nell'esito. Se l'attività non è prevista, consulta le raccomandazioni per la correzione descritte in dettaglio in [Riparazione di un bucket S3 potenzialmente compromesso](#).

Argomenti

- [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

Un'API comunemente utilizzata per scovare gli oggetti S3 è stata richiamata in modo anomalo.

Gravità predefinita: bassa

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito indica che un'entità IAM ha richiamato un'API S3 per scoprire i bucket S3 nel tuo ambiente, ad esempio `ListObjects`. Questo tipo di attività è associata alla fase di scoperta di un attacco, in cui un aggressore raccoglie informazioni per determinare se l'AWS ambiente in uso è suscettibile a un attacco più ampio. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello di machine learning (ML) GuardDuty di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle

richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta [Dettagli sugli esiti](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Discovery:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per scoprire risorse in un AWS ambiente è stata richiamata da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail relativi ai dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è generalmente associata alla fase di scoperta di un attacco, quando un avversario sta raccogliendo informazioni sull'ambiente in uso. AWS A titolo di esempio si possono menzionare `GetObjectAcl` e `ListObjects`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Discovery:S3/MaliciousIPCaller.Custom

Un'API S3 è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'API S3, come `GetObjectAcl` o `ListObjects`, è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Discovery:S3/TorIPCaller

Un'API S3 è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'API S3, come `GetObjectAcl` o `ListObjects`, è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Questo tipo di attività è associata alla fase di scoperta di un attacco, in cui un aggressore raccoglie informazioni per determinare se l'AWS ambiente in uso è suscettibile a un attacco più ampio. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle AWS risorse dell'utente con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Exfiltration:S3/AnomalousBehavior

Un'entità IAM ha richiamato un'API S3 in modo sospetto.

Gravità predefinita: alta

- Fonte dei dati: CloudTrail eventi relativi ai dati per S3

Questo esito segnala che un'entità IAM effettua chiamate API che coinvolgono un bucket S3 e questa attività differisce dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata alla fase di esfiltrazione di un attacco, in cui un utente malintenzionato tenta di raccogliere dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta [Dettagli sugli esiti](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Exfiltration:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per raccogliere dati da un AWS ambiente è stata richiamata da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail relativi ai dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di esfiltrazione in cui un avversario cerca di raccogliere dati dalla tua rete. A titolo di esempio si possono menzionare GetObject e CopyObject.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Impact:S3/AnomalousBehavior.Delete

Un'entità IAM ha richiamato un'API S3 che tenta di eliminare i dati in modo sospetto.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo risultato indica che un'entità IAM nel tuo AWS ambiente sta effettuando chiamate API che coinvolgono un bucket S3 e questo comportamento è diverso dalla linea di base stabilita da tale entità. La chiamata API utilizzata in questa attività è associata a un attacco che tenta di eliminare i dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta [Dettagli sugli esiti](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Ti consigliamo di controllare il contenuto del tuo bucket S3 per determinare se la versione precedente dell'oggetto può o deve essere ripristinata.

Impact:S3/AnomalousBehavior.Permission

Un'API comunemente utilizzata per impostare le autorizzazioni della lista di controllo degli accessi (ACL) è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo risultato ti informa che un'entità IAM nel tuo AWS ambiente ha aggiornato una policy o un ACL sui bucket S3 elencati. Questa modifica può esporre pubblicamente i bucket S3 a tutti gli utenti autenticati. AWS

Questa API è stata identificata come anomala dal modello di apprendimento automatico (ML) GuardDuty di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta [Dettagli sugli esiti](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Ti consigliamo di controllare il contenuto del tuo bucket S3 per assicurarti che a nessun oggetto sia stato inaspettatamente consentito l'accesso pubblico.

Impact:S3/AnomalousBehavior.Write

Un'entità IAM ha richiamato un'API S3 che tenta di scrivere i dati in modo sospetto.

Gravità predefinita: media

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo risultato indica che un'entità IAM nel tuo AWS ambiente sta effettuando chiamate API che coinvolgono un bucket S3 e questo comportamento è diverso dalla linea di base stabilita da tale

entità. La chiamata API utilizzata in questa attività è associata a un attacco che tenta di scrivere i dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello di machine learning (ML) per GuardDuty il rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta [Dettagli sugli esiti](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Ti consigliamo di controllare il contenuto del tuo bucket S3 per assicurarti che questa chiamata API non abbia scritto dati dannosi o non autorizzati.

Impact:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per manomettere dati o processi in un AWS ambiente è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di impatto in cui un avversario cerca di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS A titolo di esempio si possono menzionare PutObject e PutObjectAc1.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

PenTest:S3/KaliLinux

Un'API S3 è stata richiamata da una macchina Kali Linux.

Gravità predefinita: media

- Fonte dei dati: eventi relativi ai dati per S3 CloudTrail

Questa scoperta ti informa che una macchina che esegue Kali Linux sta effettuando chiamate all'API S3 utilizzando credenziali che appartengono al tuo account. AWS Le tue credenziali potrebbero essere compromesse. Kali Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

PenTest:S3/ParrotLinux

Un'API S3 è stata richiamata da una macchina Parrot Security Linux.

Gravità predefinita: media

- Fonte dei dati: eventi relativi ai dati per S3 CloudTrail

Questa scoperta indica che una macchina su cui è in esecuzione Parrot Security Linux sta effettuando chiamate all'API S3 utilizzando credenziali che appartengono al vostro account. AWS Le tue credenziali potrebbero essere compromesse. Parrot Security Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Questo strumento è utilizzato

anche dagli utenti malintenzionati per identificare le vulnerabilità nella configurazione EC2 e ottenere accesso non autorizzato all'ambiente AWS .

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

PenTest:S3/PentooLinux

Un'API S3 è stata richiamata da una macchina Pentoo Linux.

Gravità predefinita: media

- Fonte dei dati: CloudTrail eventi di dati per S3

Questa scoperta ti informa che una macchina che esegue Pentoo Linux sta effettuando chiamate all'API S3 utilizzando credenziali che appartengono al tuo account. AWS Le tue credenziali potrebbero essere compromesse. Pentoo Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Policy:S3/AccountBlockPublicAccessDisabled

Un'entità IAM ha richiamato un'API utilizzata per disabilitare il blocco dell'accesso pubblico S3 su un account.

Gravità predefinita: bassa

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che il blocco dell'accesso pubblico Amazon S3 è stato disabilitato a livello di account. Quando le impostazioni di S3 Block Public Access sono abilitate, vengono utilizzate per filtrare le politiche o gli elenchi di controllo degli accessi (ACLs) sui bucket come misura di sicurezza per prevenire l'esposizione pubblica involontaria dei dati.

In genere, il blocco dell'accesso pubblico S3 è disattivato nell'account per consentire l'accesso pubblico a un bucket o agli oggetti al suo interno. Quando S3 Block Public Access è disabilitato per un account, l'accesso ai bucket è controllato dalle policy o dalle impostazioni di Block Public Access a livello di bucket applicate ai singoli bucket. ACLs Questo non significa per forza che i bucket sono condivisi pubblicamente, ma che è necessario controllare le autorizzazioni applicate ai bucket per verificare che forniscano il livello di accesso appropriato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Policy:S3/BucketAnonymousAccessGranted

Un titolare IAM ha concesso l'accesso a un bucket S3 a Internet modificando le policy del bucket o. ACLs

Gravità predefinita: alta

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che il bucket S3 elencato è stato reso accessibile pubblicamente su Internet perché un'entità IAM ha modificato una policy o un'ACL per il bucket in questione.

Dopo aver rilevato una modifica alla policy o all'ACL, GuardDuty utilizza il ragionamento automatico fornito da [Zelkova](#) per determinare se il bucket è accessibile al pubblico.

Note

Se le policy di un bucket ACLs o di un bucket sono configurate per negare esplicitamente o negare tutto, questo risultato potrebbe non riflettere lo stato attuale del bucket. Questo esito non rifletterà alcuna impostazione di [Blocco dell'accesso pubblico S3](#) che potrebbe essere

stata abilitata per il tuo bucket S3. In questi casi, il valore `effectivePermission` dell'esito verrà contrassegnato come UNKNOWN.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Policy:S3/BucketBlockPublicAccessDisabled

Un'entità IAM ha richiamato un'API utilizzata per disabilitare il blocco dell'accesso pubblico S3 su un bucket.

Gravità predefinita: bassa

- CloudTrail Fonte dei dati: eventi di gestione

Questo esito segnala che il blocco dell'accesso pubblico è stato disabilitato per il bucket S3 elencato. Se abilitate, le impostazioni di S3 Block Public Access vengono utilizzate per filtrare le politiche o le liste di controllo degli accessi (ACLs) applicate ai bucket come misura di sicurezza per prevenire l'esposizione pubblica involontaria dei dati.

In genere, il blocco dell'accesso pubblico S3 è disattivato su un bucket per consentire l'accesso pubblico al bucket in questione o agli oggetti al suo interno. Quando S3 Block Public Access è disabilitato per un bucket, l'accesso al bucket è controllato dalle policy o applicato ad esso. ACLs Ciò non significa che il bucket sia condiviso pubblicamente, ma è necessario verificare le politiche e ACLs applicarle al bucket per confermare che vengano applicate le autorizzazioni appropriate.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Policy:S3/BucketPublicAccessGranted

Un responsabile IAM ha concesso l'accesso pubblico a un bucket S3 a tutti AWS gli utenti modificando le policy del bucket o. ACLs

Gravità predefinita: alta

- Fonte dei dati: eventi di gestione CloudTrail

Questo risultato indica che il bucket S3 elencato è stato esposto pubblicamente a tutti AWS gli utenti autenticati perché un'entità IAM ha modificato una policy del bucket o ACL su quel bucket S3.

Una volta rilevata una modifica alla policy o all'ACL, GuardDuty utilizza il ragionamento automatico fornito da [Zelkova](#) per determinare se il bucket è accessibile al pubblico.

Note

Se le policy di un bucket ACLs o di un bucket sono configurate per negare esplicitamente o negare tutto, questo risultato potrebbe non riflettere lo stato attuale del bucket. Questo esito non rifletterà alcuna impostazione di [Blocco dell'accesso pubblico S3](#) che potrebbe essere stata abilitata per il tuo bucket S3. In questi casi, il valore `effectivePermission` dell'esito verrà contrassegnato come UNKNOWN.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Stealth:S3/ServerAccessLoggingDisabled

La registrazione degli accessi al server S3 è stata disabilitata per un bucket.

Gravità predefinita: bassa

- CloudTrail Fonte dei dati: eventi di gestione

Questa scoperta ti informa che la registrazione degli accessi al server S3 è disabilitata per un bucket all'interno del tuo ambiente. AWS Se disabilitata, non viene creato alcun registro delle richieste Web per i tentativi di accesso al bucket S3 identificato, tuttavia, le chiamate API di gestione S3 al bucket, ad esempio, vengono comunque tracciate. [DeleteBucket](#) Se la registrazione degli eventi dei dati S3 è abilitata CloudTrail per questo bucket, le richieste web per gli oggetti all'interno del bucket verranno comunque tracciate. La disabilitazione della registrazione è una tecnica utilizzata da utenti non autorizzati per evitare il rilevamento. Per ulteriori informazioni sui log S3, consulta [Registrazione degli accessi al server S3](#) e [Opzioni di registrazione S3](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Un'API S3 è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Fonte dati: eventi di dati per S3 CloudTrail

Questo esito segnala che un'operazione API S3, ad esempio, PutObject o PutObjectAc1, è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

UnauthorizedAccess:S3/TorIPCaller

Un'API S3 è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3, come PutObject o PutObjectAcl, è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Questa scoperta può indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Tipi di risultati di protezione EKS

I seguenti risultati sono specifici delle risorse Amazon EKS e hanno un valore resource_type di EKSCluster. La gravità e i dettagli degli esiti variano in base al tipo di esito.

Per tutti i risultati relativi ai log di audit EKS, consigliamo di esaminare la risorsa in questione per determinare se l'attività è prevista o potenzialmente dannosa. Per indicazioni sulla correzione di una risorsa compromessa dei registri di controllo EKS identificata da un GuardDuty risultato, vedere.

[Correzione dei risultati della protezione EKS](#)

Note

Se questi esiti vengono generati a causa di un'attività prevista, valuta la possibilità di aggiungere una [Regole di soppressione in GuardDuty](#) per evitare avvisi futuri.

Argomenti

- [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/ContainerWithSensitiveMount](#)
- [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](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [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

Prima della versione 1.14 di Kubernetes, il `system:unauthenticated` gruppo era associato a e per impostazione predefinita. `system:discovery system:basic-user ClusterRoles` Questa associazione potrebbe consentire l'accesso non intenzionale a utenti anonimi. Gli aggiornamenti del cluster non revocano queste autorizzazioni. Anche se hai aggiornato il cluster alla versione 1.14 o successiva, le autorizzazioni in questione potrebbero essere ancora abilitate. Ti consigliamo di disassociare queste autorizzazioni dal gruppo `system:unauthenticated`. Per indicazioni sulla revoca di queste autorizzazioni, consulta le [best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide](#).

CredentialAccess:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *KubernetesUserDetails* sezione lo è *system:anonymous*, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revoca le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle [best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon](#) EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Caratteristica: log di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente *system:anonymous*. Le chiamate API effettuate da *system:anonymous* non sono autenticate.

L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

CredentialAccess:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse del cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per

determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata a tattiche

di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

DefenseEvasion:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Discovery:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata alla fase di scoperta di un attacco in cui

l'utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio.

 Per accessi non autenticati

MaliciousIPCalleri risultati non vengono generati per l'accesso non autenticato.
SuccessfulAnonymousAccessi risultati vengono generati per un accesso non autenticato o anonimo.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Discovery:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'API è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni,

se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Discovery:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata alla fase di scoperta di un attacco, quando un avversario raccoglie informazioni sul cluster Kubernetes. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Questo tipo di risultato esclude gli endpoint dell'API Health Check come `/healthz`, `/livez`, `/readyz` e `/version`

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Discovery:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è `system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare la API e revoca delle autorizzazioni, se necessario, seguendo le istruzioni riportate nelle [best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS](#). Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Execution:Kubernetes/ExecInKubeSystemPod

È stato eseguito un comando in un pod all'interno dello spazio dei nomi del **kube-system**.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che è stato eseguito un comando in un pod all'interno dello spazio dei nomi del kube-system utilizzando l'API di esecuzione Kubernetes. Lo spazio dei nomi del kube-system è predefinito e viene utilizzato principalmente per componenti a livello di sistema, come kube-dns e kube-proxy. L'esecuzione di comandi in pod o container all'interno dello spazio dei nomi del kube-system è molto rara e può indicare attività sospette.

Raccomandazioni per la correzione:

Se l'esecuzione di questo comando non è prevista, le credenziali dell'identità utente utilizzate per eseguirlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Impact:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di impatto in cui un avversario cerca di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Impact:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata a tattiche di impatto in cui un avversario cerca di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Impact:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è generalmente associata alla fase di impatto di un attacco, quando un avversario manomette le risorse del cluster. Questa attività indica che è stato autorizzato l'accesso anonimo o

non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Impact:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata a tattiche di impatto con cui un avversario cerca di manipolare, interrompere o distruggere dati all'interno del tuo ambiente AWS . Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente

e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Persistence:Kubernetes/ContainerWithSensitiveMount

È stato avviato un container con un percorso host esterno sensibile montato all'interno.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un container è stato avviato con una configurazione che includeva un percorso host sensibile con accesso in scrittura nella sezione `volumeMounts`. Ciò rende questo percorso accessibile e scrivibile dall'interno del container. Questa tecnica viene comunemente utilizzata dagli avversari per accedere al file system dell'host.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione composta da un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve essere uguale all'`imagePrefix` specificato nell'esito. Per ulteriori informazioni sulla creazione delle regole di eliminazione, consulta [Regole di eliminazione](#).

Persistence:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per mantenere l'accesso persistente a un cluster Kubernetes è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e cerca di mantenerlo.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Persistence:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per mantenere l'accesso persistente a un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e cerca di mantenerlo.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Persistence:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per ottenere autorizzazioni di alto livello per un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata alle tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster e cerca di mantenerlo. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Persistence:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per mantenere l'accesso persistente a un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e cerca di mantenerlo. Tor è un software che consente la

comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se l'utente ha segnalato l'esito nella sezione `KubernetesUserDetails` è `system:anonymous`, scopri perché all'utente anonimo è stato permesso di invocare l'API e di revocare le autorizzazioni, se necessario, seguendo le istruzioni contenute nelle [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

All'account di servizio predefinito sono stati concessi i privilegi di amministratore su un cluster Kubernetes.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che all'account di servizio predefinito per un namespace nel cluster Kubernetes sono stati concessi i privilegi di amministratore. Kubernetes crea un account di servizio predefinito per tutti gli spazi dei nomi del cluster e lo assegna automaticamente come identità ai pod che non sono stati associati esplicitamente a un altro account di servizio. Se l'account di servizio predefinito dispone di privilegi di amministratore, è possibile che vengano lanciati involontariamente pod con privilegi di amministratore. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Non utilizzare l'account di servizio predefinito per concedere autorizzazioni ai pod. Crea invece un account di servizio dedicato per ogni carico di lavoro e concedi l'autorizzazione a tale account in base alle esigenze. Per risolvere questo problema, crea account di servizio dedicati per tutti i tuoi pod e carichi di lavoro e aggiornali per migrare dall'account di servizio predefinito ai relativi account dedicati. Rimuovi quindi l'autorizzazione di amministratore dall'account di servizio predefinito. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Policy:Kubernetes/AnonymousAccessGranted

All'utente **system:anonymous** è stata concessa l'autorizzazione API su un cluster Kubernetes.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un utente del cluster Kubernetes ha creato correttamente un `ClusterRoleBinding` o `RoleBinding` per associare l'utente `system:anonymous` a un ruolo. In questo modo viene consentito l'accesso non autenticato alle operazioni API autorizzate dal ruolo. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` o al gruppo `system:unauthenticated` sul cluster e revoca l'accesso anonimo non necessario. Per ulteriori informazioni, consulta le [Best practice di sicurezza per Amazon EKS](#) nella Guida per l'utente di Amazon EKS. Se le autorizzazioni sono state concesse intenzionalmente, revoca l'accesso dell'utente che le ha concesse e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Policy:Kubernetes/ExposedDashboard

Il pannello di un cluster Kubernetes era esposto a Internet

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che il pannello Kubernetes per il cluster è stato esposto a Internet da un servizio del sistema di bilanciamento del carico. Un pannello esposto rende l'interfaccia di gestione del cluster accessibile da Internet e consente agli avversari di sfruttare eventuali lacune nell'autenticazione e nel controllo degli accessi.

Raccomandazioni per la correzione:

Assicurati di applicare autenticazione e autorizzazione avanzate sul pannello Kubernetes. Inoltre, implementa il controllo dell'accesso alla rete per limitare l'accesso al pannello da indirizzi IP specifici.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Policy:Kubernetes/KubeflowDashboardExposed

Il pannello Kubeflow di un cluster Kubernetes era esposto a Internet

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che il pannello Kubeflow per il cluster è stato esposto a Internet da un servizio del sistema di bilanciamento del carico. Un pannello Kubeflow esposto rende l'interfaccia di gestione dell'ambiente Kubeflow accessibile da Internet e consente agli avversari di sfruttare eventuali lacune nell'autenticazione e nel controllo degli accessi.

Raccomandazioni per la correzione:

Assicurati di applicare autenticazione e autorizzazione avanzate sul pannello Kubeflow. Inoltre, implementa il controllo dell'accesso alla rete per limitare l'accesso al pannello da indirizzi IP specifici.

Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Un container privilegiato con accesso a livello root è stato avviato sul cluster Kubernetes.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un container privilegiato è stato avviato sul cluster Kubernetes utilizzando un'immagine che non era mai stata utilizzata per avviare container privilegiati nel cluster. Un container privilegiato ha accesso di livello root all'host. Gli avversari possono avviare container privilegiati come tattica di escalation dei privilegi per accedere all'host e quindi comprometterlo.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Un'API Kubernetes comunemente utilizzata per accedere a segreti è stata richiamata in modo anomalo.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API anomala volta a recuperare segreti sensibili del cluster è stata richiamata da un utente Kubernetes del cluster. L'API osservata è comunemente associata a tattiche di accesso alle credenziali che possono portare a un'escalation dei privilegi e a ulteriori accessi all'interno del cluster. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali AWS sono compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster EKS e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello di ML tiene traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes nel cluster e assicurati che siano tutte necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Nel cluster RoleBinding ClusterRoleBinding Kubernetes è stato creato o modificato un ruolo o un namespace riservato eccessivamente permissivo.

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se un RoleBinding or ClusterRoleBinding coinvolge o, la gravità è Alta. ClusterRoles `admin` `cluster-admin`

- Caratteristica: registri di controllo EKS

Questo esito segnala che un utente del cluster Kubernetes ha creato un RoleBinding o un ClusterRoleBinding per associare un utente a un ruolo con autorizzazioni di amministratore o spazi dei nomi sensibili. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali AWS sono compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes. Queste autorizzazioni sono definite nel ruolo e nei soggetti coinvolti nel RoleBinding e nel ClusterRoleBinding. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

Execution:Kubernetes/AnomalousBehavior.ExecInPod

È stato eseguito un comando in un pod in modo anomalo.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un comando è stato eseguito in un pod utilizzando l'API di esecuzione Kubernetes. L'API di esecuzione Kubernetes consente di eseguire di comandi arbitrari in un pod. Se questo comportamento non è previsto per l'utente, lo spazio dei nomi o il pod, può indicare un errore di configurazione o che le AWS credenziali sono compromesse.

L'API osservata è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'esecuzione di questo comando non è prevista, le credenziali dell'identità utente utilizzate per eseguirlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed! PrivilegedContainer

Un carico di lavoro è stato avviato in modo anomalo con un container privilegiato.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che è stato avviato un carico di lavoro con un container privilegiato nel cluster Amazon EKS. Un container privilegiato ha accesso di livello root all'host. Gli utenti non autorizzati possono avviare container privilegiati come tattica di escalation dei privilegi prima per accedere all'host, poi per comprometterlo.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività degli utenti legate all'API e all'immagine del container all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

**Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!
ContainerWithSensitiveMount**

Un carico di lavoro è stato implementato in modo anomalo con un percorso host sensibile montato al suo interno.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che un carico di lavoro è stato avviato con un container che includeva un percorso host sensibile nella sezione `volumeMounts`. Ciò rende questo percorso potenzialmente accessibile e scrivibile dall'interno del container. Questa tecnica viene comunemente utilizzata dagli utenti non autorizzati per accedere al file system dell'host.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività degli utenti legate all'API e all'immagine del container all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Un carico di lavoro è stato avviato in modo anomalo.

Gravità predefinita: bassa*

Note

La gravità predefinita è bassa. Tuttavia, se il carico di lavoro contiene un nome immagine potenzialmente sospetto, ad esempio uno strumento di test di penetrazione (pen-test) noto,

o un container che esegue un comando potenzialmente sospetto all'avvio, come i comandi di shell (interprete di comandi) inversa, questo tipo di esito verrà considerato di gravità media.

- Caratteristica: registri di controllo EKS

Questo esito segnala che un carico di lavoro Kubernetes, ad esempio un'attività API, nuove immagini del container o una configurazione rischiosa del carico di lavoro, è stato creato o modificato in modo anomalo all'interno del cluster Amazon EKS. Gli utenti non autorizzati possono avviare container come tattica per eseguire un codice arbitrario prima per accedere all'host, poi per comprometterlo.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività degli utenti legate all'API e all'immagine del container all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Un ruolo altamente permissivo o ClusterRole è stato creato o modificato in modo anomalo.

Gravità predefinita: bassa

- Caratteristica: registri di controllo EKS

Questo esito segnala che un'operazione API anomala volta a creare un Role o un ClusterRole con autorizzazioni eccessive è stata chiamata da un utente Kubernetes del cluster Amazon EKS. Gli attori possono utilizzare la creazione di ruoli con autorizzazioni avanzate per non utilizzare ruoli incorporati simili a quelli di amministratore ed evitare il rilevamento. Le autorizzazioni eccessive possono portare a un'escalation dei privilegi, all'esecuzione di codice in modalità remota e al potenziale controllo di uno spazio dei nomi o di un cluster. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster Amazon EKS e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni definite in Role o ClusterRole per assicurarti che tutte le autorizzazioni siano necessarie e segui i principi del privilegio minimo. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un utente ha verificato la propria autorizzazione di accesso in modo anomalo.

Gravità predefinita: bassa

- Caratteristica: registri di controllo EKS

Questo esito segnala che un utente del cluster Kubernetes ha verificato correttamente se sono consentite o meno le autorizzazioni avanzate note che possono portare a un'escalation dei privilegi e all'esecuzione di codice in modalità remota. Ad esempio, `kubectl auth can-i` è un comando comune utilizzato per verificare le autorizzazioni di un utente. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono state compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster Amazon EKS e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'autorizzazione oggetto della verifica e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes per assicurarti che siano tutte necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Se AWS le tue credenziali sono compromesse, consulta. [Riparazione delle credenziali potenzialmente compromesse AWS](#)

GuardDuty Tipi di risultati del monitoraggio del runtime

Amazon GuardDuty genera i seguenti risultati di Runtime Monitoring per indicare potenziali minacce in base al comportamento a livello di sistema operativo degli host e contenitori Amazon EC2 nei cluster Amazon EKS, nei carichi di lavoro Fargate e Amazon ECS e nelle istanze Amazon EC2.

 Note

I tipi di esiti del monitoraggio del runtime EKS si basano sui log di runtime raccolti dagli host. I log contengono campi, come i percorsi dei file, che potrebbero essere controllati da un utente malintenzionato. Questi campi sono inclusi anche nei risultati per fornire un contesto di runtime. GuardDuty Quando si elaborano i risultati del Runtime Monitoring all'esterno della GuardDuty console, è necessario ripulire i campi di ricerca. Ad esempio, puoi codificare in HTML i campi degli esiti quando li visualizzi su una pagina Web.

Argomenti

- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [Backdoor:Runtime/C&CAActivity.B](#)
- [UnauthorizedAccess:Runtime/TorRelay](#)
- [UnauthorizedAccess:Runtime/TorClient](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/DropPoint](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Backdoor:Runtime/C&CAActivity.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/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/KernelModuleLoaded](#)

CryptoCurrency:Runtime/BitcoinTool.B

Un'istanza Amazon EC2 o un container eseguono una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta interrogando un indirizzo IP associato a un'attività correlata alla criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 o un container per estrarre o gestire criptovaluta o se questi elementi sono altrimenti coinvolti nell'attività di blockchain, l'esito `CryptoCurrency:Runtime/BitcoinTool.B` potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di esito con un valore di `CryptoCurrency:Runtime/BitcoinTool.B`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta [Regole di eliminazione](#).

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Backdoor:Runtime/C&CActivity.B

Un'istanza Amazon EC2 o un container eseguono una query su un IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore all'interno del tuo AWS ambiente sta interrogando un indirizzo IP associato a un server di comando e controllo (C&C) noto. L'istanza elencata o il container potrebbero essere potenzialmente compromessi. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è un insieme di dispositivi connessi a Internet che possono includere server PCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche emettere comandi per avviare un attacco Denial of Service (S) distribuito. DDo

Note

Se l'IP su cui viene eseguita una query è correlato a log4j, i campi dell'esito associato includeranno i valori seguenti:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

UnauthorizedAccess:Runtime/TorRelay

L'istanza Amazon EC2 o un container stabiliscono connessioni a una rete Tor come relè Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

UnauthorizedAccess:Runtime/TorClient

L'istanza Amazon EC2 o un container stabiliscono connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che l'istanza EC2 o il container sono stati compromessi e fungono da client su una rete Tor. Questa scoperta potrebbe indicare un accesso non autorizzato alle AWS risorse dell'utente con l'intento di nascondere la vera identità dell'aggressore.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/BlackholeTraffic

Un'istanza Amazon EC2 o un container tentano di comunicare con l'indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente potrebbe essere compromesso perché sta tentando di comunicare con l'indirizzo IP di un buco nero (o sink hole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/DropPoint

Un'istanza Amazon EC2 o un container tentano di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta tentando di comunicare con un indirizzo IP di un host remoto noto per contenere credenziali e altri dati rubati acquisiti dal malware.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta interrogando un nome di dominio associato a Bitcoin o ad altre attività legate alla criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo al fine di riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 o container per estrarre o gestire criptovaluta o se questi elementi sono altrimenti coinvolti nell'attività di blockchain, l'esito CryptoCurrency:Runtime/BitcoinTool.B!DNS potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti

consigliamo di impostare una regola di soppressione per questo risultato. La regola di eliminazione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta [Regole di eliminazione](#).

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Backdoor:Runtime/C&CActivity.B!DNS

Un'istanza Amazon EC2 o un container eseguono una query su nome di dominio associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore all'interno del tuo AWS ambiente sta interrogando un nome di dominio associato a un server di comando e controllo (C&C) noto. L'istanza EC2 elencata o il container potrebbero essere compromessi. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è un insieme di dispositivi connessi a Internet che può includere server PCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche emettere comandi per avviare un attacco Denial of Service (S) distribuito. DDo

Note

Se il nome di dominio su cui è stata eseguita la query è relativo a log4j, i campi dell'esito associato includeranno i valori seguenti:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

 Note

Per verificare come GuardDuty genera questo tipo di risultato, puoi effettuare una richiesta DNS dalla tua istanza (utilizzando `dig` per Linux o `nslookup` per Windows) su un dominio di test. `guarddutyactivityb.com`

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/BlackholeTraffic!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio che è reindirizzato a un indirizzo IP di un buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore nel tuo AWS ambiente potrebbe essere compromesso perché sta interrogando un nome di dominio che viene reindirizzato a un indirizzo IP di buco nero. I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/DropPoint!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta interrogando un nome di dominio di un host remoto noto per contenere credenziali e altri dati rubati acquisiti da malware.

L'agente di GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/DGADomainRequest.C!DNS

Un'istanza Amazon EC2 o un container eseguono una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 o un container compromessi.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore dell' AWS ambiente sta cercando di interrogare i domini DGA (Domain Generation Algorithm). La tua risorsa potrebbe essere stata compromessa.

DGAs vengono utilizzati per generare periodicamente un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

Note

Questo risultato si basa su domini DGA noti provenienti dai feed di intelligence sulle minacce. GuardDuty

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/DriveBySourceTraffic!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio di un host remoto che è l'origine nota di attacchi di download drive-by.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore dell'AWS ambiente potrebbe essere compromesso perché interroga il nome di dominio di un host remoto che è una fonte nota di attacchi drive-by download. Si tratta di download di software non voluti da Internet che possono avviare l'installazione automatica di virus, spyware o malware.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Trojan:Runtime/PhishingDomainRequest!DNS

Un'istanza Amazon EC2 o un container eseguono una query su domini implicati in attacchi di phishing.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta cercando di interrogare un dominio coinvolto in attacchi di phishing. I domini di phishing sono configurati da individui che fingono di essere un'istituzione legittima allo scopo di indurre gli utenti a fornire dati sensibili come informazioni personali, coordinate bancarie, informazioni di carte di credito e password. L'istanza EC2 o il container potrebbero tentare di recuperare dati sensibili archiviati su un sito Web di phishing oppure di configurare un sito Web di phishing. L'istanza EC2 o il container potrebbero essere compromessi.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Impact:Runtime/AbusedDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio a bassa reputazione associato a domini noti in abuso.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione associato a domini o indirizzi IP noti in modo abusivo. Esempi di domini in abuso sono i nomi di dominio di primo livello (TLD) e i nomi di dominio di secondo livello (2LD) che offrono registrazioni gratuite di sottodomini e provider DNS dinamici. Gli autori delle minacce tendono a utilizzare questi servizi per registrare domini gratuitamente o a basso costo. I domini a bassa reputazione di questa categoria possono anche essere domini scaduti che vengono sostituiti con l'indirizzo IP di parcheggio di un registrar e quindi potrebbero non essere più attivi. Un IP di parcheggio è il luogo in cui un registrar indirizza il traffico verso domini che non sono stati collegati ad alcun servizio. L'istanza Amazon EC2 elencata o il container potrebbero essere compromessi poiché gli autori delle minacce utilizzano comunemente questi registrar o servizi per la distribuzione di malware e C&C.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Impact:Runtime/BitcoinDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio a bassa reputazione associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione associato a Bitcoin o ad altre attività legate alle criptovalute. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 o il container per estrarre o gestire criptovaluta o se tali risorse sono altrimenti coinvolte nell'attività di blockchain, questo esito potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di Impact:Runtime/BitcoinDomainRequest.Reputation. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta [Regole di eliminazione](#).

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Impact:Runtime/MaliciousDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un dominio a bassa reputazione associato a domini dannosi noti.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione associato a domini o indirizzi IP dannosi noti. Ad esempio, i domini possono essere associati a un indirizzo IP sinkhole noto. I domini sinkhole sono domini che sono stati precedentemente controllati da un autore di minacce e se vengono inoltrate richieste a questi domini può significare che l'istanza è compromessa. Questi domini possono anche essere correlati a campagne dannose note o algoritmi di generazione di domini.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità che sia dannoso.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Impact:Runtime/SuspiciousDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio a bassa reputazione di natura sospetta a causa della sua età o della scarsa popolarità.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza EC2 elencata o sul contenitore all'interno del tuo AWS ambiente sta interrogando un nome di dominio di bassa reputazione che si sospetta sia dannoso. Le caratteristiche osservate di questo dominio erano coerenti con i domini dannosi osservati in precedenza. Tuttavia, il nostro modello di reputazione non è stato in grado di collegarlo in modo definitivo a una minaccia nota. Questi domini vengono in genere osservati per la prima volta o ricevono una quantità di traffico ridotta.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

UnauthorizedAccess:Runtime/MetadataDNSRebind

Un'istanza Amazon EC2 o un container eseguono ricerche DNS che vengono risolte nel servizio di metadati dell'istanza.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Note

Attualmente, questo tipo di risultato è supportato solo per AMD64 l'architettura.

Questo risultato ti informa che un processo in esecuzione sull'istanza EC2 elencata o su un contenitore nel tuo AWS ambiente sta interrogando un dominio che si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). Una query DNS di questo tipo può indicare che l'istanza è la destinazione di una tecnica di rebinding DNS. Questa tecnica può essere utilizzata per ottenere metadati da un'istanza EC2, incluse le credenziali IAM a essa associate.

Il rebinding DNS implica l'inganno di un'applicazione in esecuzione sull'istanza EC2 per caricare i dati restituiti da un URL, dove il nome di dominio nell'URL si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). In questo modo l'applicazione accede ai metadati EC2 e, possibilmente, li rende disponibili all'utente malintenzionato.

Puoi accedere ai metadati EC2 utilizzando il rebinding DNS solo se l'istanza EC2 esegue un'applicazione vulnerabile che consente l'iniezione di URL oppure se qualcuno accede all'URL in un browser Web in esecuzione sull'istanza EC2.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. GuardDuty Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

In risposta a questo esito, devi valutare se è presente un'applicazione vulnerabile in esecuzione sull'istanza EC2 o sul container o se qualcuno ha utilizzato un browser per accedere al dominio identificato nell'esito. Se la causa principale è un'applicazione vulnerabile, procedi alla correzione della vulnerabilità. Se qualcuno ha navigato nel dominio identificato, blocca il dominio o impedisce agli utenti di accedervi. Se ritieni che l'esito sia correlato a uno dei due casi precedenti, [Revoca la sessione associata all'istanza EC2](#).

Alcuni AWS clienti associano intenzionalmente l'indirizzo IP dei metadati a un nome di dominio sui propri server DNS autoritativi. Se questo è il caso del tuo ambiente, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. Il secondo criterio di filtro deve essere il Dominio richiesta DNS o l'ID immagine del container. Il valore del Dominio richiesta DNS deve corrispondere al dominio mappato all'indirizzo IP dei metadati (169.254.169.254). Per informazioni sulla creazione di regole di eliminazione, consulta [Regole di eliminazione](#).

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/NewBinaryExecuted

È stato eseguito un file binario appena creato o modificato di recente in un container.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato indica che è stato eseguito un file binario appena creato o modificato di recente in un contenitore. Ti consigliamo di mantenere i container non modificabili in fase di runtime. Inoltre, i file binari, gli script e le librerie non devono essere creati o modificati durante il ciclo di vita del container. Questo comportamento indica che un utente malintenzionato ha ottenuto l'accesso al container, ha scaricato ed eseguito malware o altro software come parte della potenziale violazione. Sebbene questo tipo di attività possa essere indice di una violazione, è anche un modello di utilizzo comune. Pertanto, GuardDuty utilizza meccanismi per identificare i casi sospetti di questa attività e genera questo tipo di risultati solo per i casi sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Per identificare il processo di modifica e il nuovo file binario, visualizza i dettagli del processo di modifica e i dettagli del processo

I dettagli del processo di modifica sono inclusi nel

`service.runtimeDetails.context.modifyingProcess` campo del codice JSON di ricerca o in Processo di modifica nel pannello dei dettagli di ricerca. Per questo tipo di ricerca, il processo di modifica è `/usr/bin/dpkg` identificato dal `service.runtimeDetails.context.modifyingProcess.executablePath` campo del JSON di ricerca o come parte del processo di modifica nel pannello dei dettagli del risultato.

I dettagli del file binario nuovo o modificato eseguito sono inclusi nella sezione JSON

`service.runtimeDetails.process` di ricerca o nella sezione Process in Runtime details. Per questo tipo di ricerca, il file binario nuovo o modificato è `/usr/bin/python3.8`, come indicato dal campo `service.runtimeDetails.process.executablePath` (Percorso eseguibile).

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un processo all'interno di un container comunica con il daemon Docker utilizzando il socket Docker.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Il socket Docker è un socket di dominio Unix utilizzato da daemon Docker (dockerd) per comunicare con i propri client. Un client può eseguire varie operazioni, come la creazione di container comunicando con il daemon Docker tramite il socket Docker. È sospetto che un processo del container acceda al socket Docker. Un processo contenitore può uscire dal contenitore e ottenere un accesso a livello di host comunicando con il socket Docker e creando un contenitore privilegiato.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/RuncContainerEscape

È stato rilevato un tentativo di fuga dal container tramite runC.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

RunC è il runtime di container di basso livello utilizzato dai runtime di container di alto livello, come Docker e Containerd, per generare ed eseguire contenitori. RunC viene sempre eseguito con i privilegi di root perché deve eseguire l'operazione di basso livello di creazione di un contenitore. Un autore di minacce può ottenere l'accesso a livello di host modificando o sfruttando una vulnerabilità nel binario RunC.

Questa scoperta rileva la modifica del binario RunC e i potenziali tentativi di sfruttare le seguenti vulnerabilità RunC:

- [CVE-2019-5736](#)— Lo sfruttamento di CVE-2019-5736 implica la sovrascrittura del binario RunC dall'interno di un contenitore. Questa scoperta viene richiamata quando il binario RunC viene modificato da un processo all'interno di un contenitore.

- [CVE-2024-21626](#)— Lo sfruttamento di CVE-2024-21626 implica l'impostazione della directory di lavoro corrente (CWD) o di un contenitore su un descrittore di file aperto. `/proc/self/fd/FileDescriptor` Questo risultato viene richiamato quando viene rilevato un processo contenitore con una directory di lavoro corrente sotto `/proc/self/fd/`, ad esempio. `/proc/self/fd/7`

Questo esito può indicare che un malintenzionato ha tentato di sfruttare uno dei seguenti tipi di container:

- Un nuovo container con un'immagine controllata dall'utente malintenzionato.
- Un container esistente accessibile all'attore con autorizzazioni di scrittura sul binario runC a livello di host.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

È stato rilevato un tentativo di fuga dal container tramite il CGroups release agent.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che è stato rilevato un tentativo di modificare un file dell'agente di rilascio del gruppo di controllo (cgroup). Linux utilizza i gruppi di controllo (cgroup) per limitare, tenere in considerazione e isolare l'utilizzo delle risorse di una raccolta di processi. Ogni cgroup ha un file dell'agente di rilascio (`release_agent`), uno script che Linux esegue quando termina un processo all'interno del cgroup. Il file dell'agente di rilascio viene sempre eseguito a livello di host. Un autore di minacce all'interno di un container può sfuggire all'host scrivendo comandi arbitrari nel file dell'agente di rilascio che appartiene a un cgroup. Al termine di un processo all'interno di questo cgroup, i comandi scritti dall'autore vengono eseguiti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

DefenseEvasion:Runtime/ProcessInjection.Proc

In un container o in un'istanza Amazon EC2 è stata rilevata un'iniezione di processo utilizzando il file system proc.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Il file system proc (procfs) è un particolare file system in Linux che presenta la memoria virtuale del processo come file. Il percorso di questo file è `/proc/PID/mem`, in cui PID è l'ID univoco del processo. Un autore di minacce può scrivere su questo file per iniettare codice nel processo. Questo esito identifica potenziali tentativi di scrittura sul file in questione.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

DefenseEvasion:Runtime/ProcessInjection.Ptrace

In un container o in un'istanza Amazon EC2 è stata rilevata un'iniezione di processo utilizzando la chiamata di sistema ptrace.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Un processo può utilizzare la chiamata di sistema ptrace per iniettare codice in un altro processo. Questo esito identifica un potenziale tentativo di iniettare codice in un processo utilizzando la chiamata di sistema ptrace.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

In un container o in un'istanza Amazon EC2 è stata rilevata un'iniezione di processo tramite scrittura diretta nella memoria virtuale.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Un processo può utilizzare una chiamata di sistema, ad esempio `process_vm_writew`, per iniettare codice direttamente nella memoria virtuale di un altro processo. Questo esito identifica un potenziale tentativo di iniettare codice in un processo utilizzando una chiamata di sistema per scrivere nella memoria virtuale del processo stesso.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/ReverseShell

Un processo in un container o in un'istanza Amazon EC2 ha creato una shell (interprete di comandi) inversa.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Una shell (interprete di comandi) inversa è una sessione di shell creata su una connessione avviata dall'host di destinazione all'host dell'attore, ossia l'opposto di una normale shell (interprete di comandi), che viene invece avviata dall'host dell'attore all'host di destinazione. Gli autori delle minacce creano una shell (interprete di comandi) inversa per eseguire comandi sulla destinazione dopo aver ottenuto l'accesso iniziale. Questa scoperta identifica connessioni a shell inversa potenzialmente sospette.

GuardDuty esamina l'attività e il contesto di runtime correlati e genera questo tipo di risultato solo quando l'attività e il contesto associati risultano insoliti o sospetti. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Il GuardDuty security agent monitora gli eventi da più fonti. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli della ricerca nella GuardDuty console. Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

DefenseEvasion:Runtime/FilelessExecution

Un processo in un container o in un'istanza Amazon EC2 esegue codice dalla memoria.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala un processo eseguito utilizzando un file eseguibile in memoria su disco. Si tratta di una tecnica comune di evasione della difesa in cui il file eseguibile dannoso non viene scritto sul disco per eludere il rilevamento basato sulla scansione del file system. Sebbene questa sia una tecnica utilizzata dal malware, presenta anche alcuni casi d'uso legittimi. Uno degli esempi è un compilatore just-in-time (JIT) che scrive codice compilato in memoria e lo esegue dalla memoria.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Impact:Runtime/CryptoMinerExecuted

Un container o un'istanza Amazon EC2 eseguono un file binario associato a un'attività attività di mining di criptovalute.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato indica che un processo in esecuzione sull'istanza o sul contenitore EC2 elencato nell'AWS ambiente in uso sta eseguendo un file binario associato a un'attività di mining di criptovalute. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console e vedi [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/NewLibraryLoaded

Una libreria appena creata o modificata di recente è stata caricata da un processo all'interno di un container.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che una libreria è stata creata o modificata all'interno di un container durante il runtime e caricata da un processo in esecuzione all'interno del container. La best practice è quella di mantenere i container non modificabili in fase di runtime e di non creare o modificare i file binari, gli script e le librerie durante il ciclo di vita del container. Il caricamento di una libreria appena creata o modificata in un container può indicare attività sospette. Questo comportamento indica che un utente malintenzionato ha potenzialmente ottenuto l'accesso al container e che ha scaricato ed eseguito malware o altro software come parte della potenziale compromissione. Sebbene questo tipo di attività possa essere indice di una violazione, è anche un modello di utilizzo comune. Pertanto, GuardDuty utilizza meccanismi per identificare i casi sospetti di questa attività e genera questo tipo di risultati solo per i casi sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un processo all'interno di un container ha montato un file system host in fase di runtime.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Diverse tecniche di evasione da un container prevedono il montaggio di un file system host al suo interno in fase di runtime. Questo esito segnala che un processo all'interno di un container ha potenzialmente tentato di montare un file system host, il che potrebbe indicare un tentativo di sfuggire all'host.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un processo ha utilizzato chiamate di sistema **userfaultfd** per gestire errori di pagina nello spazio utente.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

In genere, gli errori di pagina vengono gestiti dal kernel nello spazio corrispondente. Tuttavia, la chiamata di sistema `userfaultfd` consente a un processo di gestire gli errori di pagina su un file system nello spazio utente. Questa funzionalità è utile perché abilita l'implementazione di file system nello spazio utente. D'altra parte, può anche essere usata da un processo potenzialmente dannoso per interrompere il kernel dallo spazio utente. L'interruzione del kernel tramite la chiamata di sistema

`userfaultfd` è una tecnica di sfruttamento comune volta a estendere le finestre di gara durante lo sfruttamento delle condizioni di gara del kernel. L'utilizzo di `userfaultfd` può quindi indicare attività sospette sull'istanza Amazon Elastic Compute Cloud (Amazon EC2).

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/SuspiciousTool

Un container o un'istanza Amazon EC2 eseguono un file binario o uno script che vengono spesso utilizzati in scenari di sicurezza offensivi come il test di penetrazione.

Gravità predefinita: variabile

La gravità di questa constatazione può essere elevata o bassa, a seconda che lo strumento sospetto rilevato sia considerato a duplice uso o destinato esclusivamente a un uso offensivo.

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che uno strumento sospetto è stato eseguito su un'istanza o contenitore EC2 all'interno del tuo ambiente. AWS Ciò include gli strumenti utilizzati nelle attività di test di penetrazione, noti anche come strumenti backdoor, scanner di rete e sniffer di rete. Tutti questi strumenti possono essere utilizzati in contesti benigni, ma sono spesso utilizzati anche da autori di minacce con intenzioni malevole. L'osservazione di strumenti di sicurezza offensivi potrebbe indicare che l'istanza o il contenitore EC2 associato è stato compromesso.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/SuspiciousCommand

Un comando sospetto è stato eseguito su un'istanza Amazon EC2 o un container indicativo di una violazione.

Gravità predefinita: variabile

A seconda dell'impatto del modello dannoso osservato, la gravità di questo tipo di rilevamento potrebbe essere bassa, media o alta.

- Funzionalità: monitoraggio del runtime

Questo risultato indica che è stato eseguito un comando sospetto e indica che un'istanza Amazon EC2 o un contenitore nel AWS tuo ambiente è stato compromesso. Ciò potrebbe significare che un file è stato scaricato da una fonte sospetta e quindi eseguito oppure che un processo in esecuzione mostra un pattern dannoso noto nella riga di comando. Ciò indica inoltre che il malware è in esecuzione sul sistema.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Note

Gli argomenti della riga di comando del processo possono contenere dati sensibili. Per proteggere i dati sensibili, i risultati del monitoraggio del

GuardDuty runtime non includono argomenti completi della riga di comando. `Service.RuntimeDetails.Context.CommandLineExample` fornisce invece un esempio rappresentativo dello schema della riga di comando che ha generato il risultato.

DefenseEvasion:Runtime/SuspiciousCommand

Un comando è stato eseguito sull'istanza Amazon EC2 elencata o su un container, tenta di modificare o disabilitare un meccanismo di difesa Linux, come un firewall o servizi di sistema essenziali.

Gravità predefinita: variabile

A seconda del meccanismo di difesa modificato o disabilitato, la gravità di questo tipo di esito può essere alta, media o bassa.

- Funzionalità: monitoraggio del runtime

Questo esito ti informa che è stato eseguito un comando che tenta di nascondere un attacco ai servizi di sicurezza del sistema locale. Ciò include azioni come disabilitare il firewall Unix, modificare le tabelle IP locali, rimuovere le voci crontab, disabilitare un servizio locale o assumere il controllo della funzione `LDPreload`. Qualsiasi modifica è altamente sospetta e un potenziale indicatore di compromissione. Pertanto, questi meccanismi rilevano o impediscono ulteriori violazioni del sistema.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

DefenseEvasion:Runtime/PtraceAntiDebugging

Un processo in un container o in un'istanza Amazon EC2 ha eseguito una misura anti-debugging utilizzando la chiamata di sistema ptrace.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questo risultato mostra che un processo in esecuzione sull'istanza Amazon EC2 elencata o su un contenitore all'interno del tuo AWS ambiente ha utilizzato la chiamata di sistema ptrace con l'opzione. PTRACE_TRACEME Questa attività causerebbe il distacco di un debugger collegato al processo in esecuzione. Se non è collegato alcun debugger, non ha effetto. Tuttavia, l'attività di per sé solleva sospetti. Ciò potrebbe indicare che sul sistema è in esecuzione un malware. Il malware utilizza spesso tecniche anti-debugging per eludere l'analisi e queste tecniche possono essere rilevate in fase di runtime.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/MaliciousFileExecuted

Un file eseguibile dannoso noto è stato eseguito su un'istanza Amazon EC2 o un container.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un file eseguibile dannoso noto è stato eseguito su un'istanza Amazon EC2 o su un contenitore all'interno AWS del tuo ambiente. Questo è un forte indicatore del fatto che l'istanza o il container è stato potenzialmente compromesso e che il malware è stato eseguito.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Execution:Runtime/SuspiciousShellCreated

Un servizio di rete o un processo accessibile dalla rete su un'istanza Amazon EC2 o in un contenitore ha avviato un processo shell interattivo.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un servizio accessibile in rete su un'istanza Amazon EC2 o in un contenitore all'interno del tuo AWS ambiente ha lanciato una shell interattiva. In determinate circostanze, questo scenario può indicare un comportamento successivo allo sfruttamento. Le shell interattive consentono agli aggressori di eseguire comandi arbitrari su un'istanza o un container compromessi.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini. È possibile visualizzare le informazioni sul processo accessibili in rete nei dettagli del processo principale.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/ElevationToRoot

Un processo in esecuzione sull'istanza o sul contenitore Amazon EC2 elencato ha assunto i privilegi di root.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'Amazon EC2 elencato o nel contenitore elencato all'interno del AWS tuo ambiente ha assunto i privilegi di root a causa di un'esecuzione binaria insolita o `setuid` sospetta. Ciò indica che un processo in esecuzione è stato potenzialmente compromesso, per l'istanza EC2, a causa di un exploit o di uno sfruttamento. `setuid` Utilizzando i privilegi di root, l'aggressore può potenzialmente eseguire comandi sull'istanza o sul contenitore.

Sebbene GuardDuty sia progettato per non generare questo tipo di risultati per attività che richiedono l'uso regolare del `sudo` comando, lo genererà quando identificherà l'attività come insolita o sospetta.

GuardDuty esamina l'attività e il contesto di runtime correlati e genera questo tipo di risultato solo quando l'attività e il contesto associati sono insoliti o sospetti.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Discovery:Runtime/SuspiciousCommand

È stato eseguito un comando sospetto su un'istanza Amazon EC2 o in un container, che consente a un utente malintenzionato di ottenere informazioni sul sistema locale, sull'infrastruttura AWS circostante o sull'infrastruttura del container.

Gravità predefinita: bassa

Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza o sul contenitore Amazon EC2 elencato nel AWS tuo ambiente ha eseguito un comando che potrebbe fornire a un utente malintenzionato informazioni cruciali per far avanzare potenzialmente l'attacco. È possibile che siano state recuperate le seguenti informazioni:

- Sistema locale, ad esempio configurazione utente o rete,
- Altre AWS risorse e autorizzazioni disponibili, oppure
- l'infrastruttura Kubernetes come servizi e pod.

L'istanza Amazon EC2 o il contenitore elencato nei dettagli del risultato potrebbero essere stati compromessi.

L'agente GuardDuty runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Puoi trovare i dettagli sul comando sospetto nel campo `service.runtimeDetails.context` del JSON degli esiti. Un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione dei processi, è disponibile nei risultati per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Persistence:Runtime/SuspiciousCommand

È stato eseguito un comando sospetto su un'istanza Amazon EC2 o in un container, che consente a un utente malintenzionato di mantenere l'accesso e il controllo nel tuo ambiente. AWS

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza Amazon EC2 elencata o in un contenitore all'interno del AWS tuo ambiente ha eseguito un comando sospetto. Il comando installa un metodo di persistenza che consente al malware di funzionare senza interruzioni o consente a un utente malintenzionato di accedere continuamente all'istanza o al tipo di risorsa del contenitore potenzialmente compromessi. Ciò potrebbe potenzialmente significare che un servizio di sistema è stato installato o modificato, che è `crontab` stato modificato o che un nuovo utente è stato aggiunto alla configurazione del sistema.

GuardDuty esamina l'attività e il contesto di runtime correlati e genera questo tipo di risultato solo quando l'attività e il contesto associati sono insoliti o sospetti.

L'istanza Amazon EC2 o il contenitore elencato nei dettagli del risultato potrebbero essere stati compromessi.

L'agente GuardDuty di runtime monitora gli eventi da più risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Puoi trovare i dettagli sul comando sospetto nel campo `service.runtimeDetails.context` del JSON degli esiti. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

PrivilegeEscalation:Runtime/SuspiciousCommand

È stato eseguito un comando sospetto su un'istanza Amazon EC2 o in un contenitore, che consente a un utente malintenzionato di aumentare i privilegi.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo risultato ti informa che un processo in esecuzione sull'istanza Amazon EC2 elencata o in un contenitore all'interno del AWS tuo ambiente ha eseguito un comando sospetto. Il comando tenta di eseguire l'escalation dei privilegi, che consente a un avversario di eseguire attività con privilegi elevati.

GuardDuty esamina l'attività e il contesto di runtime correlati e genera questo tipo di risultato solo quando l'attività e il contesto associati sono insoliti o sospetti.

L'istanza Amazon EC2 o il contenitore elencato nei dettagli del risultato potrebbero essere stati compromessi.

L'agente GuardDuty di runtime monitora gli eventi da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

DefenseEvasion:Runtime/KernelModuleLoaded

Un modulo del kernel è stato caricato su un'istanza Amazon EC2, indicando un tentativo di ottenere l'accesso a livello di kernel.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito indica che un modulo del kernel è stato caricato sull'istanza EC2 elencata. Poiché i moduli del kernel dispongono dei privilegi più elevati a livello di sistema (ring 0), ciò potrebbe indicare che un autore di minacce ha ottenuto l'accesso a livello di kernel. Questo livello di accesso consente il controllo completo del sistema.

L'agente GuardDuty runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console. Se applicabile, nei risultati è disponibile un contesto aggiuntivo, comprese le informazioni sul processo e sulla derivazione del processo, per ulteriori indagini.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta [Riparazione degli esiti del monitoraggio del runtime](#).

Protezione da malware per tipi di ricerca EC2

GuardDuty Malware Protection for EC2 fornisce un'unica funzionalità di Malware Protection for EC2 che individua tutte le minacce rilevate durante la scansione di un'istanza EC2 o di un carico di lavoro di un container. L'esito include il numero totale di rilevamenti effettuati durante la scansione e, in base alla gravità, fornisce dettagli sulle 32 minacce rilevate principali. A differenza di altri GuardDuty risultati, i risultati di Malware Protection for EC2 non vengono aggiornati quando viene nuovamente scansionata la stessa istanza EC2 o lo stesso carico di lavoro dello stesso container.

Per ogni scansione che rileva il malware viene generato un nuovo risultato di Malware Protection for EC2. I risultati di Malware Protection for EC2 includono informazioni sulla scansione corrispondente che ha prodotto il risultato e sul GuardDuty risultato che ha avviato la scansione. In questo modo, la correlazione tra il comportamento sospetto e il malware rilevato è più semplice.

Note

Quando GuardDuty rileva attività dannose su un carico di lavoro di un container, Malware Protection for EC2 non genera un risultato a livello EC2.

I seguenti risultati sono specifici di GuardDuty Malware Protection for EC2.

Argomenti

- [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

È stato rilevato un file dannoso su un'istanza EC.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Caratteristica: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi sull'istanza EC2 elencata all'interno dell'ambiente in uso. AWS Questa istanza elencata potrebbe essere compromessa. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Execution:ECS/MaliciousFile

È stato rilevato un file dannoso su un cluster ECS.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi su un carico di lavoro di un container che appartiene a un cluster ECS. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il container appartenente al cluster ECS potrebbe essere compromesso. Per ulteriori informazioni, consulta [Riparazione di un cluster ECS potenzialmente compromesso](#).

Execution:Kubernetes/MaliciousFile

È stato rilevato un file dannoso su un cluster Kubernetes.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Caratteristica: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi su un carico di lavoro di container che appartiene a un cluster Kubernetes. Se questo cluster è gestito da EKS, i dettagli degli esiti forniranno informazioni aggiuntive sulla risorsa EKS interessata. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Execution:Container/MaliciousFile

È stato rilevato un file dannoso in un container autonomo.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi sul carico di lavoro di un container e non sono state identificate informazioni sul cluster. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta [Riparazione di un contenitore autonomo potenzialmente compromesso](#).

Execution:EC2/SuspiciousFile

È stato rilevato un file sospetto su un'istanza EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un'istanza EC2. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo SuspiciousFile indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se ti aspetti di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Execution:ECS/SuspiciousFile

È stato rilevato un file sospetto su un cluster ECS.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un contenitore che appartiene a un cluster ECS. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se prevedi di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il container appartenente al cluster ECS potrebbe essere compromesso. Per ulteriori informazioni, consulta [Riparazione di un cluster ECS potenzialmente compromesso](#).

Execution:Kubernetes/SuspiciousFile

È stato rilevato un file sospetto su un cluster Kubernetes.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un contenitore che appartiene a un cluster Kubernetes. Se questo cluster è gestito da EKS, i dettagli degli esiti forniranno informazioni aggiuntive sull'EKS interessato. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se prevedi di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta [Correzione dei risultati della protezione EKS](#).

Execution:Container/SuspiciousFile

È stato rilevato un file sospetto in un container autonomo.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un contenitore senza informazioni sul cluster. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo SuspiciousFile indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se prevedi di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta [Riparazione di un contenitore autonomo potenzialmente compromesso](#).

Protezione da malware per tipo di ricerca S3

GuardDuty genera un risultato solo quando rileva una potenziale minaccia alla sicurezza nel tuo Account AWS. Un risultato di Malware Protection for S3 indica che l'oggetto caricato che ha avviato la scansione antimalware contiene un file potenzialmente dannoso.

Affinché Amazon GuardDuty generi un risultato nel tuo Account AWS, abilita entrambi GuardDuty e Malware Protection for S3. La migliore pratica è abilitare prima Malware Protection for S3 GuardDuty

e poi. Se per te questo ordine è diverso, assicurati di abilitarlo GuardDuty prima che un oggetto S3 venga caricato nel tuo bucket protetto.

Note

GuardDuty non riesce a generare un risultato per un oggetto S3 che è stato scansionato prima dell'attivazione. GuardDuty Per scansionare un oggetto S3 esistente, puoi caricarlo di nuovo.

Object:S3/MaliciousFile

È stato rilevato un file dannoso su un oggetto S3 scansionato.

Gravità predefinita: alta

- Funzionalità: protezione da malware per S3

Questo esito indica che una scansione antimalware ha rilevato che l'oggetto S3 elencato è dannoso. Per ulteriori informazioni, consulta la sezione Minacce rilevate nel pannello dei dettagli dei risultati.

Raccomandazione correttiva:

Se questo esito è inaspettato, l'oggetto S3 è potenzialmente dannoso. Per informazioni sulle procedure di riparazione consigliate, vedere. [Riparazione di un oggetto S3 potenzialmente dannoso](#)

Tipi di ricerca di Malware Protection for Backup

GuardDuty Malware Protection for Backup fornisce un'unica ricerca per tutte le minacce rilevate durante la scansione della risorsa richiesta. L'esito include il numero totale di rilevamenti effettuati durante la scansione e, in base alla gravità, fornisce dettagli sulle 32 minacce rilevate principali. A differenza di altri GuardDuty risultati, i risultati di Malware Protection for Backup non vengono aggiornati quando la stessa risorsa viene nuovamente analizzata. Per ogni scansione che rileva il malware viene generato un nuovo risultato di Malware Protection for Backup.

I seguenti risultati sono specifici di GuardDuty Malware Protection for Backup.

Argomenti

- [Execution:EC2/MaliciousFile!Snapshot](#)
- [Execution:EC2/MaliciousFile!AMI](#)
- [Execution:EC2/MaliciousFile!RecoveryPoint](#)
- [Execution:S3/MaliciousFile!RecoveryPoint](#)

Execution:EC2/MaliciousFile!Snapshot

È stato rilevato un file dannoso in un'istantanea EBS.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: Protezione da malware per il backup

Questo risultato indica che una scansione di GuardDuty Malware Protection for Backup ha rilevato uno o più file dannosi in un'istantanea EBS all'interno dell'ambiente. Per ulteriori informazioni, consulta la sezione Minacce rilevate nel pannello dei dettagli dell'esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista, lo snapshot potrebbe essere compromesso. Per ulteriori informazioni, consulta [Correzione di uno snapshot EBS potenzialmente compromesso](#).

Execution:EC2/MaliciousFile!AMI

È stato rilevato un file dannoso su un'AMI EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: Protezione da malware per il backup

Questo risultato indica che una scansione di GuardDuty Malware Protection for Backup ha rilevato uno o più file dannosi in un'AMI all'interno dell'ambiente in uso. Per ulteriori informazioni, consulta la sezione Minacce rilevate nel pannello dei dettagli dell'esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'AMI potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un AMI EC2 potenzialmente compromesso](#).

Execution:EC2/MaliciousFile!RecoveryPoint

Un file dannoso è stato rilevato in un punto di ripristino AWS di Backup EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: Protezione da malware per il backup

Questo risultato indica che una scansione di GuardDuty Malware Protection for Backup ha rilevato uno o più file dannosi in un punto di ripristino EC2 all'interno dell'ambiente. Il punto di ripristino interessato potrebbe essere uno snapshot EBS o un'AMI EC2. Per ulteriori informazioni, consulta la sezione Minacce rilevate nel pannello dei dettagli dell'esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il punto di ripristino EC2 potrebbe essere compromesso. Per ulteriori informazioni, consulta [Riparazione di un punto di ripristino EC2 potenzialmente compromesso](#).

Execution:S3/MaliciousFile!RecoveryPoint

È stato rilevato un file dannoso in un punto di ripristino AWS di Backup S3.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: Protezione da malware per il backup

Questo risultato indica che una scansione di GuardDuty Malware Protection for Backup ha rilevato uno o più oggetti dannosi in un punto di ripristino S3 all'interno dell'ambiente. Per ulteriori informazioni, consulta la sezione Minacce rilevate nel pannello dei dettagli dell'esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il punto di ripristino S3 potrebbe essere compromesso. Per ulteriori informazioni, consulta [Riparazione di un punto di ripristino S3 potenzialmente compromesso](#).

GuardDuty Tipi di risultati della protezione RDS

GuardDuty RDS Protection rileva un comportamento anomalo di accesso sull'istanza del database. I seguenti risultati sono specifici per [Database Amazon Aurora, Amazon RDS e Aurora Limitless](#)

[supportati](#) e avranno un tipo di risorsa pari a o. RDSDBInstance RDSLimitlessDB La gravità e i dettagli dei risultati saranno diversi in base al tipo di risultato.

Argomenti

- [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](#)

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account in modo anomalo.

Gravità predefinita: variabile

Note

A seconda del comportamento anomalo associato a questo esito, la gravità predefinita può essere bassa, media e alta.

- **Bassa:** se il nome utente associato a questo esito ha effettuato l'accesso da un indirizzo IP associato a una rete privata.
- **Media:** se il nome utente associato a questo esito ha effettuato l'accesso da un indirizzo IP pubblico.
- **Alta:** se viene individuata una serie di tentativi di accesso falliti da indirizzi IP pubblici, indicativo di policy di accesso troppo permissive.

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo risultato indica che è stato osservato un accesso anomalo riuscito a un database RDS nel tuo ambiente. AWS Ciò può indicare che un utente che non era mai stato rilevato in precedenza ha effettuato l'accesso a un database RDS per la prima volta. Uno scenario comune consiste nell'accesso da parte di un utente interno a un database a cui accedono le applicazioni a livello di programmazione, ma non i singoli utenti.

Questo accesso riuscito è stato identificato come anomalo dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutti gli eventi di accesso al database nel tuo [Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati](#) e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sugli eventi di accesso potenzialmente insoliti, consulta [Anomalie basate sull'attività di accesso RDS](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, ti consigliamo di modificare la password dell'utente del database e di esaminare i log di audit disponibili per le attività eseguite dall'utente anomalo. Gli esiti di gravità media e alta possono indicare che la policy di accesso al database è troppo permissiva e che le credenziali dell'utente potrebbero essere state esposte o compromesse. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti](#).

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Uno o più tentativi di accesso insoliti falliti sono stati osservati su un database RDS del tuo account.

Gravità predefinita: bassa

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo risultato indica che sono stati osservati uno o più accessi anomali non riusciti su un database RDS nell'ambiente in uso. AWS Un tentativo di accesso fallito da indirizzi IP pubblici può indicare che il database RDS del tuo account è stato oggetto di un tentativo di attacco di forza bruta da parte di un utente potenzialmente malintenzionato.

Questi accessi non riusciti sono stati identificati come anomali dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutti gli eventi di accesso al database nel tuo [Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati](#) e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sulle attività di accesso RDS potenzialmente insolite, consulta [Anomalie basate sull'attività di accesso RDS](#).

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che il database è esposto pubblicamente o che la policy di accesso al database è troppo permissiva. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti](#).

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account da un indirizzo IP pubblico in modo anomalo dopo una serie di tentativi di accesso insoliti falliti.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo risultato indica che è stato osservato un accesso anomalo indicativo del successo della forza bruta su un database RDS dell'ambiente in uso. AWS Prima di un accesso anomalo riuscito, è stata osservata una serie di tentativi di accesso insoliti falliti. Ciò indica che l'utente e la password associati al database RDS del tuo account potrebbero essere stati compromessi e che un utente potenzialmente malintenzionato potrebbe aver effettuato l'accesso al database RDS.

Questo accesso con forza bruta riuscito è stato identificato come anomalo dal modello di apprendimento automatico per il GuardDuty rilevamento delle anomalie (ML). Il modello di ML valuta tutti gli eventi di accesso al database nel tuo [Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati](#) e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che

ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sulle attività di accesso RDS potenzialmente insolite, consulta [Anomalie basate sull'attività di accesso RDS](#).

Raccomandazioni per la correzione:

Questa attività indica che le credenziali del database potrebbero essere state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente potenzialmente compromesso. Una serie di tentativi di accesso insoliti falliti indica che la policy di accesso al database è troppo permissiva o che il database potrebbe essere stato esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti](#).

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo risultato indica che si è verificata un'attività di accesso RDS riuscita da un indirizzo IP associato a un'attività dannosa nota nell'ambiente in uso. AWS Ciò indica che l'utente e la password associati al database RDS del tuo account potrebbero essere stati compromessi e che un utente potenzialmente malintenzionato potrebbe aver effettuato l'accesso al database RDS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che le credenziali dell'utente sono state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente compromesso. Questa attività può anche indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti](#).

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Un indirizzo IP associato a un'attività dannosa nota ha tentato di accedere a un database RDS del tuo account, senza riuscirci.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo risultato indica che un indirizzo IP associato a un'attività dannosa nota ha tentato di accedere a un database RDS nell' AWS ambiente in uso, ma non è riuscito a fornire il nome utente o la password corretti. Ciò indica che un utente potenzialmente malintenzionato potrebbe tentare di compromettere il database RDS del tuo account.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti](#).

Discovery:RDS/MaliciousIPCaller

Un database RDS del tuo account è stato sottoposto a probing da un indirizzo IP associato a un'attività dannosa nota, ma non è stato effettuato alcun tentativo di autenticazione.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo risultato indica che un indirizzo IP associato a un'attività dannosa nota ha rilevato un database RDS nell' AWS ambiente in uso, sebbene non sia stato effettuato alcun tentativo di accesso. Ciò può indicare che un utente potenzialmente malintenzionato è alla ricerca di un'infrastruttura accessibile pubblicamente.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti](#).

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un utente ha effettuato correttamente l'accesso a un database RDS nel tuo ambiente AWS dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente anonimo.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che le credenziali dell'utente sono state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente compromesso. Questa attività può anche indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti](#).

CredentialAccess:RDS/TorIPCaller.FailedLogin

Un indirizzo IP Tor ha tentato di accedere a un database RDS del tuo account, senza riuscirci.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questa scoperta ti informa che un indirizzo IP del nodo di uscita Tor ha tentato di accedere a un database RDS nel tuo AWS ambiente, ma non è riuscito a fornire il nome utente o la password corretti. Tor è un software per abilitare la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente anonimo.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti](#).

Discovery:RDS/TorIPCaller

Un database RDS del tuo account è stato sottoposto a probing dall'indirizzo IP di un nodo di uscita Tor, ma non è stato effettuato alcun tentativo di autenticazione.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un database RDS nel tuo ambiente AWS è stato sottoposto a probing dall'indirizzo IP di un nodo di uscita Tor, anche se non è stato effettuato alcun tentativo di accesso. Ciò può indicare che un utente potenzialmente malintenzionato è alla ricerca di infrastrutture accessibili pubblicamente. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente potenzialmente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire

il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta [Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti](#).

Tipi di esiti della Protezione Lambda

Questa sezione descrive i tipi di risultati specifici AWS Lambda delle tue risorse e per i quali sono resourceType elencati comeLambda. Per tutti gli esiti di Lambda, ti consigliamo di esaminare la risorsa in questione e determinare se si comporta nel modo previsto. Se l'attività è autorizzata, puoi utilizzare le [Regole di eliminazione](#) o gli [Elenchi di indirizzi IP affidabili](#) e gli elenchi minacce per prevenire notifiche false positive per quella risorsa.

Se l'attività non è prevista, la best practice di sicurezza consiste nel presupporre che Lambda sia stata potenzialmente compromessa e seguire le raccomandazioni per la correzione.

Argomenti

- [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

Una funzione Lambda esegue una query su un indirizzo IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questa scoperta indica che una funzione Lambda elencata nell' AWS ambiente in uso sta interrogando un indirizzo IP associato a un server di comando e controllo (C&C) noto. La funzione Lambda associata all'esito generato è potenzialmente compromessa. I server C&C sono computer che inviano comandi ai membri di una botnet.

Una botnet è un insieme di dispositivi connessi a Internet, che può includere server PCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un Distributed Denial of Service.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

CryptoCurrency:Lambda/BitcoinTool.B

Una funzione Lambda esegue una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questa scoperta ti informa che la funzione Lambda elencata nel AWS tuo ambiente sta interrogando un indirizzo IP associato a Bitcoin o ad altre attività legate alla criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle funzioni Lambda per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

Raccomandazioni per la correzione:

Se usi questa funzione Lambda per estrarre o gestire criptovaluta o se questa funzione è altrimenti coinvolta in un'attività di blockchain, può trattarsi di un'attività potenzialmente prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio deve utilizzare l'attributo tipo di esito con un valore di CryptoCurrency:Lambda/BitcoinTool.B. Il secondo criterio di filtro deve essere il nome della funzione Lambda coinvolta nell'attività di blockchain. Per informazioni sulla creazione di regole di eliminazione, consulta [Regole di eliminazione](#).

Se questa attività non è prevista, la funzione Lambda è potenzialmente compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

Trojan:Lambda/BlackholeTraffic

Una funzione Lambda tenta di comunicare con l'indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questa scoperta indica che una funzione Lambda elencata nell' AWS ambiente in uso sta tentando di comunicare con l'indirizzo IP di un buco nero (o di un buco nel pozzo). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host. La funzione Lambda elencata è potenzialmente compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

Trojan:Lambda/DropPoint

Una funzione Lambda tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo risultato indica che una funzione Lambda elencata nell' AWS ambiente in uso sta tentando di comunicare con un indirizzo IP di un host remoto noto per contenere credenziali e altri dati rubati acquisiti da malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Una funzione Lambda stabilisce connessioni a un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questa scoperta ti informa che una funzione Lambda nel AWS tuo ambiente sta comunicando con un indirizzo IP incluso in un elenco di minacce che hai caricato. In GuardDuty, un [elenco di minacce](#) è composto da indirizzi IP dannosi noti. GuardDuty genera risultati basati sugli elenchi di minacce caricati. È possibile visualizzare i dettagli dell'elenco delle minacce nei dettagli di ricerca sulla GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

UnauthorizedAccess:Lambda/TorClient

Una funzione Lambda stabilisce connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questa scoperta ti informa che una funzione Lambda nel AWS tuo ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi Authority fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che la funzione Lambda è stata potenzialmente compromessa e al momento funge da client su una rete Tor.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

UnauthorizedAccess:Lambda/TorRelay

Una funzione Lambda stabilisce connessioni a una rete Tor come relè Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questa scoperta ti informa che una funzione Lambda nel AWS tuo ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta consente l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di una funzione Lambda potenzialmente compromessa](#).

Tipi di esiti ritirati

Un risultato è una notifica che contiene dettagli su un potenziale problema di sicurezza rilevato da GuardDuty . Per informazioni sulle modifiche importanti ai tipi di risultati, inclusi i tipi di GuardDuty risultati appena aggiunti o ritirati, vedere. [Cronologia dei documenti per Amazon GuardDuty](#)

I seguenti tipi di risultati vengono ritirati e non sono più generati da. GuardDuty

Important

Non puoi riattivare i tipi di ricerca ritirati GuardDuty .

Argomenti

- [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](#)

Exfiltration:S3/ObjectRead.Unusual

Un'entità IAM ha richiamato un'API S3 in modo sospetto.

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo risultato indica che un'entità IAM nel tuo AWS ambiente sta effettuando chiamate API che coinvolgono un bucket S3 e che differiscono dalla linea di base stabilita da tale entità. La chiamata API utilizzata in questa attività è associata alla fase di esfiltrazione di un attacco, in cui un utente malintenzionato tenta di raccogliere dati. Questa attività è sospetta perché il modo in cui l'entità IAM

ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Impact:S3/PermissionsModification.Unusual

Un'entità IAM ha richiamato un'API per modificare le autorizzazioni su una o più risorse S3.

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo esito segnala che un'entità IAM effettua chiamate API progettate per modificare le autorizzazioni su uno o più bucket o oggetti nel tuo ambiente AWS . Questa operazione può essere eseguita da un utente malintenzionato per consentire la condivisione di informazioni al di fuori dell'account. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Impact:S3/ObjectDelete.Unusual

Un'entità IAM ha richiamato un'API utilizzata per eliminare i dati in un bucket S3.

Gravità predefinita: media*

 Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è Alta.

Questo risultato indica che un'entità IAM specifica nel tuo AWS ambiente sta effettuando chiamate API progettate per eliminare i dati nel bucket S3 elencato eliminando il bucket stesso. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Discovery:S3/BucketEnumeration.Unusual

Un'entità IAM ha richiamato un'API S3 utilizzata per scoprire i bucket S3 all'interno della rete.

Gravità predefinita: media*

 Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo esito indica che un'entità IAM ha richiamato un'API S3 per scoprire i bucket S3 nel tuo ambiente, ad esempio `ListBuckets`. Questo tipo di attività è associata alla fase di scoperta di un attacco, in cui un utente malintenzionato raccoglie informazioni per determinare se l'AWS ambiente in uso è suscettibile a un attacco più ampio. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta [Riparazione di un bucket S3 potenzialmente compromesso](#).

Persistence:IAMUser/NetworkPermissions

Un'entità IAM ha richiamato un'API comunemente utilizzata per modificare le autorizzazioni di accesso alla rete per i gruppi di sicurezza, le rotte e nel tuo account.

ACLs AWS

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo risultato indica che un principale specifico (Utente root dell'account AWS ruolo o utente IAM) nell' AWS ambiente mostra un comportamento diverso dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le impostazioni di configurazione della rete vengono modificate in circostanze sospette, ad esempio quando un principale richiama l'API `CreateSecurityGroup` senza averlo mai fatto in precedenza. Gli utenti malintenzionati spesso tentano di modificare i gruppi di sicurezza per consentire un determinato traffico in entrata su varie porte e migliorare la capacità di accedere all'istanza EC2.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Persistence:IAMUser/ResourcePermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le politiche di accesso di sicurezza di varie risorse del tuo Account AWS

Gravità predefinita: media*

 Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo risultato indica che un principale specifico (Utente root dell'account AWS ruolo o utente IAM) nell' AWS ambiente mostra un comportamento diverso dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo risultato viene attivato quando viene rilevata una modifica alle policy o alle autorizzazioni associate alle AWS risorse, ad esempio quando un principale nell' AWS ambiente richiama l'PutBucketPolicyAPI senza precedenti. Alcuni servizi, come Amazon S3, supportano le autorizzazioni collegate alle risorse che concedono a uno o più principali di accedere alla risorsa. Con le credenziali rubate, gli utenti malintenzionati possono modificare le policy collegate a una risorsa per potervi accedere.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Persistence:IAMUser/UserPermissions

Un principale ha richiamato un'API comunemente utilizzata per aggiungere, modificare o eliminare utenti, gruppi o politiche IAM nel tuo account. AWS

Gravità predefinita: media*

 Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo risultato indica che un principale specifico (Utente root dell'account AWS ruolo o utente IAM) nell' AWS ambiente mostra un comportamento diverso dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo risultato è dovuto a modifiche sospette alle autorizzazioni relative all'utente nell'AWS ambiente in uso, ad esempio quando un responsabile dell'AWS ambiente richiama l'AttachUserPolicyAPI senza precedenti. Gli utenti malintenzionati possono utilizzare le credenziali rubate per creare nuovi utenti, aggiungere policy di accesso agli utenti esistenti o creare chiavi di accesso per massimizzare l'accesso a un account, anche se il punto di accesso originale è chiuso. Ad esempio, il proprietario dell'account potrebbe accorgersi del furto di un determinato utente IAM o di una password ed eliminarli dall'account. Tuttavia, potrebbero non eliminare altri utenti creati da un amministratore creato in modo fraudolento, lasciando il loro account accessibile all'aggressore. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

PrivilegeEscalation:IAMUser/AdministrativePermissions

Un principale ha tentato di assegnare una policy molto permissiva a se stessa.

Gravità predefinita: bassa*

Note

La gravità di questo esito è bassa se il tentativo di escalation dei privilegi non è andato a buon fine e media in caso contrario.

Questo risultato indica che un'entità IAM specifica nell'AWS ambiente in uso mostra un comportamento che può essere indicativo di un attacco di escalation dei privilegi. Questo esito viene attivato quando un utente o un ruolo IAM tentano di autoassegnarsi una policy molto permissiva. Se l'utente o il ruolo in questione non è destinato a disporre di privilegi amministrativi, le credenziali dell'utente potrebbero essere compromesse o le autorizzazioni del ruolo potrebbero non essere configurate correttamente.

Gli utenti malintenzionati utilizzeranno le credenziali rubate per creare nuovi utenti, aggiungere policy di accesso agli utenti esistenti o creare chiavi di accesso per massimizzare l'accesso a un account, anche se il punto di accesso originale è chiuso. Ad esempio, il proprietario dell'account potrebbe notare che una determinata credenziale di un utente IAM è stata rubata ed eliminata dall'account, ma

potrebbe non eliminare altri utenti creati da un principale amministratore creato in modo fraudolento, lasciando i loro account AWS ancora accessibili all'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Recon:IAMUser/NetworkPermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le autorizzazioni di accesso alla rete per i gruppi di sicurezza, le route e l'account dell'utente. ACLs AWS

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è Alta.

Questo risultato indica che un principale specifico (Utente root dell'account AWS ruolo o utente IAM) nell' AWS ambiente mostra un comportamento diverso dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le autorizzazioni di accesso alle risorse nel tuo AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale ha richiamato l'API `DescribeInstances` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali di cui già dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Recon:IAMUser/ResourcePermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le politiche di accesso di sicurezza di varie risorse dell'account. AWS

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo risultato indica che un principale specifico (Utente root dell'account AWS ruolo o utente IAM) nell' AWS ambiente mostra un comportamento diverso dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le autorizzazioni di accesso alle risorse nel tuo AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale ha richiamato l'API `DescribeInstances` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali di cui già dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Recon:IAMUser/UserPermissions

Un principale ha richiamato un'API comunemente utilizzata per aggiungere, modificare o eliminare utenti, gruppi o policy IAM nel tuo account. AWS

Gravità predefinita: media*

 Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo risultato viene attivato quando le autorizzazioni degli utenti nell' AWS ambiente in uso vengono rilevate in circostanze sospette. Ad esempio, se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) ha richiamato l'API `ListInstanceProfilesForRole` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali di cui già dispone.

Questo risultato indica che uno specifico preside nell' AWS ambiente in uso mostra un comportamento diverso dalla linea di base stabilita. Questo principal non ha mai chiamato questa API in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

ResourceConsumption:IAMUser/ComputeResources

Un principale ha chiamato un'API comunemente utilizzata per avviare risorse di calcolo come istanze EC.

Gravità predefinita: media*

 Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo esito viene generato quando le istanze EC2 nell'account elencato all'interno del tuo ambiente AWS vengono avviate in circostanze sospette. Questo risultato indica che un principale specifico nell' AWS ambiente in uso mostra un comportamento diverso dalla linea di base stabilita, ad

esempio se un principale (Utente root dell'account AWS un ruolo IAM o un utente IAM) ha richiamato l'`RunInstancesAPI` senza precedenti. Questa attività potrebbe essere un'indicazione che un utente malintenzionato sta utilizzando credenziali rubate per rubare tempo di calcolo (possibilmente per il mining di criptovalute o il password cracking). Può anche indicare che un utente malintenzionato utilizza un'istanza EC2 nel tuo AWS ambiente e le relative credenziali per mantenere l'accesso al tuo account.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

Stealth:IAMUser/LoggingConfigurationModified

Un preside ha richiamato un'API comunemente utilizzata per interrompere la CloudTrail registrazione, eliminare i log esistenti ed eliminare in altro modo le tracce di attività nell'account. AWS

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo esito viene attivato quando la configurazione della registrazione nell'account AWS elencato all'interno del tuo ambiente viene modificata in circostanze sospette. Questo risultato indica che un principale specifico nell' AWS ambiente in uso mostra un comportamento diverso dalla linea di base stabilita, ad esempio se un principale (Utente root dell'account AWS un ruolo IAM o un utente IAM) ha richiamato l'`StopLoggingAPI` senza precedenti. Ciò può indicare il tentativo di un utente malintenzionato di eliminare le tracce della sua attività.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:IAMUser/ConsoleLogin

È stato rilevato un accesso insolito alla console da parte di un responsabile del tuo AWS account.

Gravità predefinita: media*

Note

La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando AWS credenziali temporanee create su un'istanza, la gravità del risultato è elevata.

Questo esito viene generato quando una connessione alla console viene rilevata in circostanze sospette. Ad esempio, se un principale che non ha precedenti in tal senso ha richiamato l'ConsoleLogin API da un never-before-used client o da una posizione insolita. Potrebbe trattarsi di un'indicazione dell'utilizzo di credenziali rubate per accedere al tuo AWS account o di un utente valido che accede all'account in modo non valido o meno sicuro (ad esempio, non tramite una VPN approvata).

Questa scoperta indica che un principio specifico nel vostro AWS ambiente mostra un comportamento diverso dalla linea di base stabilita. Questo principale non ha mai eseguito connessioni con questa applicazione client da questo specifico percorso in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

UnauthorizedAccess:EC2/TorIPCaller

Un'istanza EC2 sta ricevendo connessioni in entrata da un nodo di uscita Tor.

Gravità predefinita: media

Questo risultato ti informa che un'istanza EC2 nel tuo AWS ambiente riceve connessioni in entrata da un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Questa scoperta può indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Backdoor:EC2/XORDDOS

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP associato al malware XOR S. DDo

Gravità predefinita: alta

Questo risultato indica che un'istanza EC2 nel tuo AWS ambiente sta tentando di comunicare con un indirizzo IP associato al malware XOR DDoS. L'istanza EC2 potrebbe essere compromessa. XOR DDoS è un malware Trojan che dirotta i sistemi Linux. Per accedere al sistema, lancia un attacco di forza bruta allo scopo di scoprire la password dei servizi SSH (Secure Shell) su Linux. Dopo aver acquisito le credenziali SSH e aver effettuato correttamente l'accesso, utilizza i privilegi di utente root per eseguire uno script che scarica e installa XOR S. DDo. Questo malware viene quindi utilizzato come parte di una botnet per lanciare attacchi Distributed Denial of Service (DDoS) contro altri obiettivi.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

Behavior:IAMUser/InstanceLaunchUnusual

Un utente ha avviato un tipo insolito di istanza EC2.

Gravità predefinita: alta

Questo risultato indica che un utente specifico nell' AWS ambiente in uso mostra un comportamento diverso dalla linea di base stabilita. Questo utente non ha mai avviato un'istanza EC2 di questo tipo in precedenza. Le tue credenziali di accesso potrebbero essere compromesse.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

CryptoCurrency:EC2/BitcoinTool.A

Un'istanza EC2 sta comunicando con pool di mining di bitcoin.

Gravità predefinita: alta

Questo risultato ti informa che un'istanza EC2 nel tuo AWS ambiente sta comunicando con i pool di mining Bitcoin. Nel settore del mining di criptovalute, un pool di mining designa il raggruppamento delle risorse dei minatori che condividono la loro potenza di elaborazione su una rete per condividere la ricompensa in funzione del loro contributo alla risoluzione di un blocco. Se l'istanza EC2 non è utilizzata per il mining di bitcoin, potrebbe essere compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

UnauthorizedAccess:IAMUser/UnusualASNCaller

Un'API è stata chiamata da un indirizzo IP di una rete inabituale.

Gravità predefinita: alta

Questo risultato ti informa che determinate attività sono state richiamate da un indirizzo IP di una rete insolita. Questa rete non è mai stata osservata nello storico di utilizzo di AWS dell'utente specificato. Questa attività può includere un accesso alla console, un tentativo di avviare un'istanza EC2, di creare un nuovo utente IAM, di modificare i privilegi AWS , ecc. Ciò può indicare un accesso non autorizzato alle tue risorse. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).

GuardDuty ricerca dei tipi in base alle risorse potenzialmente interessate

Le pagine seguenti sono classificate in base al tipo di risorsa potenzialmente interessata associata a un risultato: GuardDuty

- [Tipi di esiti EC2](#)
- [Tipi di esiti IAM](#)
- [tipi di ricerca delle sequenze di attacco](#)
- [Tipi di risultati di protezione S3](#)
- [Tipi di risultati di protezione EKS](#)
- [Tipi di risultati del monitoraggio del runtime](#)
- [Protezione da malware per tipi di ricerca EC2](#)
- [Protezione da malware per tipo di ricerca S3](#)
- [Tipi di ricerca di Malware Protection for Backup](#)
- [Tipi di esiti della Protezione RDS](#)
- [Tipi di esiti della Protezione Lambda](#)

GuardDuty tipi di ricerca attivi

La tabella seguente mostra tutti i tipi di esiti attivi ordinati per origine dati o funzionalità fondamentale, a seconda dei casi. Nella tabella seguente, alcuni risultati hanno i valori della colonna Finding severity contrassegnati da un asterisco (*) o da un segno più (+):

* Questi tipi di risultati hanno una gravità variabile. Un risultato di un tipo particolare può avere una gravità diversa a seconda del contesto specifico del risultato. Per ulteriori informazioni su un tipo di risultato, consulta la descrizione dettagliata.

⁺ I risultati di EC2 che utilizzano i log di flusso VPC come fonte di dati non supportano il traffico. IPv6

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:S3/AnomalousBehavior	Simple Storage Service (Amazon S3)	CloudTrail eventi relativi ai dati per S3	Bassa
Discovery:S3/MaliciousIPCaller	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
Discovery:S3/MaliciousIPCaller.Custom	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:S3/TorIP Caller	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Media
Exfiltration:S3/AnomalousBehavior	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
Exfiltration:S3/MaliciousIPCaller	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
Impact:EC2/MaliciousDomainRequest.Custom	Amazon EC2	Log DNS	Media
Impact:S3/AnomalousBehavior.Delete	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
Impact:S3/AnomalousBehavior.Permission	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
Impact:S3/AnomalousBehavior.Write	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Media
Impact:S3/MaliciousIPCaller	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
PenTest:S3/KaliLinux	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Media
PenTest:S3/ParrotLinux	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Media
PenTest:S3/PentoolLinux	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Media
UnauthorizedAccess:S3/TorIPCaller	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Simple Storage Service (Amazon S3)	CloudTrail eventi di dati per S3	Elevata
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Media
CredentialAccess:IAMUser/CompromisedCredentials	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Elevata
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Media
DefenseEvasion:IAMUser/BedrockLoggingDisabled	IAM	CloudTrail eventi di gestione	Media
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Bassa
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Elevata
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Elevata
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Media
PenTest:IAMUser/KaliLinux	IAM	CloudTrail eventi di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PenTest:IAMUser/Pa rrotLinux	IAM	CloudTrail eventi di gestione	Media
PenTest:IAMUser/Pe ntoolLinux	IAM	CloudTrail eventi di gestione	Media
Persistence:IAMUser/ AnomalousBehavior	IAM	CloudTrail eventi di gestione	Media
Stealth:IAMUser/Pa sswordPolicyChange	IAM	CloudTrail eventi di gestione	Basso [*] ₋
UnauthorizedAccess :IAMUser/InstanceC redentialExfiltrat ion.InsideAWS	IAM	CloudTrail eventi gestionali	Alto [*] ₋
Policy:S3/AccountB lockPublicAccessDi sabled	Simple Storage Service (Amazon S3)	CloudTrail eventi gestionali	Bassa
Policy:S3/BucketAn onymousAccessGrant ed	Simple Storage Service (Amazon S3)	CloudTrail eventi di gestione	Elevata
Policy:S3/BucketBl ockPublicAccessDis abled	Simple Storage Service (Amazon S3)	CloudTrail eventi di gestione	Bassa
Policy:S3/BucketPu blicAccessGranted	Simple Storage Service (Amazon S3)	CloudTrail eventi di gestione	Elevata
PrivilegeEscalatio n:IAMUser/AnomalousBehavior	IAM	CloudTrail eventi di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail eventi di gestione	Media
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail eventi di gestione	Media
Recon:IAMUser/TorIPCaller	IAM	CloudTrail eventi di gestione	Media
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail eventi di gestione	Bassa
Stealth:S3/ServerAccessLoggingDisabled	Simple Storage Service (Amazon S3)	CloudTrail eventi di gestione	Bassa
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail eventi di gestione	Media
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail eventi di gestione	Media
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail eventi di gestione	Media
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail eventi di gestione	Media
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Bassa

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Bassa
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Elevata
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Elevata
AttackSequence:EKS/CompromisedCluster	Risorse coinvolte nella sequenza di attacco	• Eventi del registro di controllo EKS • Monitoraggio del runtime per Amazon EKS • Rilevamento di malware Amazon EKS per Amazon EC2 • AWS CloudTrail eventi relativi ai dati per S3 • AWS CloudTrail eventi di gestione • Log di flusso VPC • registri delle query DNS di Route53 Resolver	Critica

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
AttackSequence:IAM/CompromisedCredentials	Risorse coinvolte nella sequenza di attacco	CloudTrail eventi di gestione	Critica
AttackSequence:S3/CompromisedData	Risorse coinvolte nella sequenza degli attacchi	CloudTrail eventi di gestione ed eventi CloudTrail relativi ai dati per S3	Critica
AttackSequence:ECS/CompromisedCluster	Risorse coinvolte nella sequenza degli attacchi	• AWS Rilevamenti di Amazon ECS Runtime (Fargate) • AWS Rilevamenti di runtime di Amazon ECS (istanze Amazon EC2) • AWS Rilevamenti di malware	Critica
AttackSequence:EC2/CompromisedInstanceGroup	Risorse coinvolte nella sequenza di attacco	• AWS Rilevamenti in fase di esecuzione di Amazon EC2 • AWS Rilevamenti di malware • Log di flusso VPC • Registri delle query DNS di Route53 Resolver	Critica
Backdoor:EC2/C&CAActivity.B!DNS	Amazon EC2	Log DNS	Elevata
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Log DNS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Log DNS	Media
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Log DNS	Elevata
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Log DNS	Elevata
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Log DNS	Bassa
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Log DNS	Media
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DropPoint!DNS	Amazon EC2	Log DNS	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Log DNS	Elevata
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Log DNS	Elevata
Execution:Container/MaliciousFile	Contenitore	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:Container/SuspiciousFile	Contenitore	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:EC2/MaliciousFile	Amazon EC2	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:EC2/SuspiciousFile	Amazon EC2	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:ECS/MaliciousFile	ECS	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:ECS/SuspiciousFile	ECS	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:Kubernetes/MaliciousFile	Kubernetes	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:Kubernetes/SuspiciousFile	Kubernetes	Protezione da malware EBS	Varia a seconda della minaccia rilevata
Execution:EC2/MaliciousFile!Snapshot	Amazon EBS	Protezione da malware per il backup	Varia a seconda della minaccia rilevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:EC2/MaliciousFile!AMI	Amazon EC2	Protezione da malware per il backup	Varia a seconda della minaccia rilevata
Execution:EC2/MaliciousFile!RecoveryPoint	AWS Backup	Protezione da malware per il backup	Varia a seconda della minaccia rilevata
Execution:S3/MaliciousFile!RecoveryPoint	AWS Backup	Protezione da malware per il backup	Varia a seconda della minaccia rilevata
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Log di controllo EKS	Media
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Log di controllo EKS	Elevata
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di controllo EKS	Elevata
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di controllo EKS	Elevata
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Log di controllo EKS	Elevata
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Log di controllo EKS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di controllo EKS	Elevata
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di controllo EKS	Elevata
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Log di controllo EKS	Elevata
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Log di controllo EKS	Bassa
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Log di controllo EKS	Media
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di controllo EKS	Media
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di controllo EKS	Media
Discovery:Kubernetes/TorIPCaller	Kubernetes	Log di controllo EKS	Media
Execution:Kubernetes/ExecInKubernetesPod	Kubernetes	Log di controllo EKS	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Log di controllo EKS	Media
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Log di controllo EKS	Bassa
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Log di controllo EKS	Elevata
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di controllo EKS	Elevata
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di controllo EKS	Elevata
Impact:Kubernetes/TorIPCaller	Kubernetes	Log di controllo EKS	Elevata
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Log di controllo EKS	Media
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Log di controllo EKS	Media
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di controllo EKS	Media
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di controllo EKS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Persistence:Kubernetes/TorIPCaller	Kubernetes	Log di controllo EKS	Media
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Log di controllo EKS	Elevata
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Log di controllo EKS	Elevata
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Log di controllo EKS	Media
Policy:Kubernetes/ExposedDashboard	Kubernetes	Log di controllo EKS	Media
PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleBindingCreated	Kubernetes	Log di controllo EKS	Medio [*]
PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleCreated	Kubernetes	Log di controllo EKS	Bassa
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Log di controllo EKS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:Kubernetes/AnonymousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Log di controllo EKS	Elevata
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Log di controllo EKS	Media
Backdoor:Lambda/C&CActivity.B	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
Trojan:Lambda/BlackholeTraffic	Lambda	Monitoraggio delle attività di rete Lambda	Media
Trojan:Lambda/DropPoint	Lambda	Monitoraggio delle attività di rete Lambda	Media
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Monitoraggio delle attività di rete Lambda	Media
UnauthorizedAccess:Lambda/TorClient	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
UnauthorizedAccess:Lambda/TorRelay	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
Object:S3/MaliciousFile	S3Object	Protezione da malware per S3	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Bassa
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Elevata
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Variabile [*] __
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Media
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Elevata
CredentialAccess:RDS/TorIPCaller.FailedLogin	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Media
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:RDS/MaliciousIPCaller	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Media
Discovery:RDS/TorIPCaller	Database Amazon Aurora, Amazon RDS e Aurora Limitless supportati	Monitoraggio delle attività di accesso RDS	Media
Backdoor:Runtime/C&CAActivity.B	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Backdoor:Runtime/C&CAActivity.B!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
CryptoCurrency:Runtime/BitcoinTool.B	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/FilelessExecution	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
DefenseEvasion:Runtime/KernelModuleLoaded	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:Runtime/ProcessInjection.Proc	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/PtraceAntiDebugging	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Bassa
DefenseEvasion:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Discovery:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Bassa
Execution:Runtime/MaliciousFileExecuted	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Execution:Runtime/NewBinaryExecuted	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Execution:Runtime/NewLibraryLoaded	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Variabile
Execution:Runtime/SuspiciousShellCreated	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Bassa
Execution:Runtime/SuspiciousTool	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Variabile
Execution:Runtime/ReverseShell	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/AbusedDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Impact:Runtime/BitcoinDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/CryptoMinerExecuted	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/MaliciousDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Impact:Runtime/SuspiciousDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Bassa

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Persistence:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/DockerSocketAccessed	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/ElevationToRoot	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/RuncContainerEscape	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
PrivilegeEscalation:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/UserfaultfdUsage	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/BlackholeTraffic	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Trojan:Runtime/BlackholeTraffic!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/DropPoint	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/DGA DomainRequest.C!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Trojan:Runtime/DriveBySourceTraffic!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Trojan:Runtime/DropPoint!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/PhishingDomainRequest!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/MetadataDNSRebind	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/TorClient	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/TorRelay	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Backdoor:EC2/C&CActivity.B	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Backdoor:EC2/DenialOfService.Dns	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Backdoor:EC2/DenialOfService.Tcp	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Backdoor:EC2/DenialOfService.Udp	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Backdoor:EC2/DenialOfService.UnusualProtocol	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Backdoor:EC2/Spambot	Amazon EC2	Registri di flusso in VPC ⁺	Media
Behavior:EC2/NetworkPortUnusual	Amazon EC2	Registri di flusso in VPC ⁺	Media
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	Registri di flusso in VPC ⁺	Media
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	Registri di flusso in VPC ⁺	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	Registri di flusso in VPC ⁺	Media
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	Registri di flusso in VPC ⁺	Media
Impact:EC2/PortSweep	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Impact:EC2/WinRMBruteForce	Amazon EC2	Registri di flusso in VPC ⁺	Basso [*]
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	Registri di flusso in VPC ⁺	Basso [*]
Recon:EC2/Portscan	Amazon EC2	Registri di flusso in VPC ⁺	Media
Trojan:EC2/BlackholeTraffic	Amazon EC2	Registri di flusso in VPC ⁺	Media
Trojan:EC2/DropPoint	Amazon EC2	Registri di flusso in VPC ⁺	Media
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	Registri di flusso in VPC ⁺	Media
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	Registri di flusso in VPC ⁺	Basso [*]

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	Registri di flusso in VPC ⁺	Basso [*] ₋
UnauthorizedAccess:EC2/TorClient	Amazon EC2	Registri di flusso in VPC ⁺	Elevata
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	Registri di flusso in VPC ⁺	Elevata

Comprendere e generare i GuardDuty risultati di Amazon

Un GuardDuty risultato rappresenta un potenziale problema di sicurezza rilevato all'interno Account AWS dei carichi di lavoro e dei dati. GuardDuty genera un risultato ogni volta che rileva attività impreviste e potenzialmente dannose nell'ambiente in uso. AWS

Puoi visualizzare e gestire i GuardDuty risultati nella pagina Findings della GuardDuty console o utilizzando le operazioni AWS CLI o l'API. Per informazioni su come gestire i GuardDuty risultati, consulta [Gestione dei GuardDuty risultati di Amazon](#).

Argomenti:

[GuardDuty formato di ricerca](#)

Comprendi il formato di GuardDuty ricerca, i tipi di ricerca e i diversi scopi delle minacce che vengono GuardDuty tracciati.

[Risultati di esempio](#)

Genera risultati di esempio nella GuardDuty console o utilizzando GuardDuty API o AWS CLI comandi. I risultati di esempio generati includono dettagli fittizi per aiutarti a comprendere i dettagli dei risultati associati a ciascun GuardDuty risultato. Questi risultati sono contrassegnati con un prefisso [ESEMPIO].

[GuardDuty Risultati dei test in account dedicati](#)

È possibile testare GuardDuty risultati specifici nel proprio ambiente. Esegui `guardduty-tester` lo script in un ambiente non di produzione Account AWS dedicato. GuardDuty Per rilevare e simulare i risultati, distribuirà determinate risorse nell'ambiente dell'utente. Questa esperienza è diversa dalla generazione di risultati campionari.

[Visualizzazione dei risultati generati nella console GuardDuty](#)

Scopri come esaminare i risultati generati nella GuardDuty console.

[Livelli di gravità dei risultati GuardDuty](#)

A ogni GuardDuty risultato è associato un livello di gravità che riflette il rischio potenziale nell'AWS ambiente in uso. Questa sezione spiega cosa significa ogni livello di gravità.

[Dettagli degli esiti](#)

Scopri i dettagli associati ai GuardDuty risultati generati nel tuo account. Questo argomento include i dettagli associati al rilevamento delle minacce di base, al rilevamento esteso delle minacce e ai piani di protezione dedicati in GuardDuty.

[GuardDuty ricerca dell'aggregazione](#)

Scopri come GuardDuty gestire più occorrenze dello stesso tipo di risultato. Aggregando gli stessi tipi di risultati rilevati, GuardDuty aggiorna il tipo di risultato originale con i dettagli più recenti.

[GuardDuty tipi di ricerca](#)

Questa sezione elenca i tipi di GuardDuty ricerca in base alla o associata [Origini dati fondamentali](#). [Caratteristica GuardDuty mappata](#) Per informazioni su ciascun tipo di risultato, seleziona il risultato desiderato per ulteriori dettagli, ad esempio la descrizione e i possibili passaggi per correggere il risultato.

GuardDuty formato di ricerca

Quando GuardDuty rileva un comportamento sospetto o imprevisto nell' AWS ambiente in uso, genera un risultato. Un risultato è una notifica che contiene i dettagli su un potenziale problema di sicurezza rilevato GuardDuty . [Visualizzazione dei risultati generati nella console GuardDuty](#) Includono informazioni sull'accaduto, sulle AWS risorse coinvolte nell'attività sospetta, sul momento in cui si è svolta l'attività e informazioni correlate che possono aiutare a comprenderne la causa principale.

Una delle informazioni più utili di questi dettagli è il tipo di risultato. La funzione del tipo di risultato è di fornire una descrizione concisa ma intelligibile del potenziale problema di sicurezza. Ad esempio, il tipo di PortProbeUnprotectedPort ricerca GuardDuty Recon:EC2/ti informa rapidamente che in qualche parte del tuo AWS ambiente, un' EC2 istanza ha una porta non protetta che un potenziale aggressore sta sondando.

GuardDuty utilizza il seguente formato per denominare i vari tipi di risultati che genera:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName. DetectionMechanism! Artefatto

Ogni parte di questo formato rappresenta un aspetto di un tipo di esito. Di seguito le spiegazioni di questi aspetti:

- **ThreatPurpose**- descrive lo scopo principale di una minaccia, un tipo di attacco o una fase di un potenziale attacco. Consulta la sezione seguente per un elenco completo degli scopi delle GuardDuty minacce.
- **ResourceTypeAffected**- descrive quale tipo di AWS risorsa viene identificato in questa scoperta come potenziale bersaglio di un avversario. Attualmente, GuardDuty può generare risultati per i tipi di risorse elencati in. [GuardDuty tipi di ricerca attivi](#)
- **ThreatFamilyName**- descrive la minaccia complessiva o la potenziale attività dannosa GuardDuty rilevata. Ad esempio, un valore di `NetworkPortUnusual` indica che un' EC2 istanza identificata nel GuardDuty risultato non ha una cronologia precedente di comunicazioni su una particolare porta remota, anch'essa identificata nel risultato.
- **DetectionMechanism**- descrive il metodo con cui è GuardDuty stato rilevato il risultato. Può essere usato per indicare una variazione di un tipo di reperto comune o un risultato che ha GuardDuty utilizzato un meccanismo specifico per la rilevazione. Ad esempio, `Backdoor:EC2/DenialOfService.Tcp` indica che il Denial of Service (DoS) è stato rilevato tramite TCP. La variante UDP è `Backdoor:/.Udp. EC2 DenialOfService`

Il valore `.Custom` indica che ha GuardDuty rilevato la scoperta in base agli elenchi di minacce personalizzati. Per ulteriori informazioni, consulta [Elenchi di entità ed elenchi di indirizzi IP](#).

Il valore di `.Reputation` indica che ha GuardDuty rilevato il risultato utilizzando un modello di punteggio di reputazione del dominio. Per ulteriori informazioni, consulta [Come AWS tiene traccia delle principali minacce alla sicurezza del cloud e aiuta a disattivarle](#).

- **Artefatto**: descrive una risorsa specifica di proprietà di uno strumento utilizzato nell'attività dannosa. Ad esempio, il DNS nel tipo di risultato `CryptoCurrency:EC2/BitcoinTool.B!DNS` indica che un' EC2 istanza Amazon sta comunicando con un dominio noto relativo a Bitcoin.

Note

Artifact è facoltativo e potrebbe non essere disponibile per GuardDuty tutti i tipi di reperti.

Scopi delle minacce

In GuardDuty una minaccia lo scopo descrive lo scopo principale di una minaccia, un tipo di attacco o una fase di un potenziale attacco. Ad esempio, alcuni scopi delle minacce, come `Backdoor`, indicano un tipo di attacco. Tuttavia, alcuni scopi delle minacce, come `Impatto`, sono in linea con le

[Tattiche MITRE ATT&CK](#). Le tattiche MITRE ATT&CK indicano diverse fasi del ciclo di attacco di un avversario. Nella versione corrente di GuardDuty, ThreatPurpose può avere i seguenti valori:

Backdoor

Questo valore indica che un avversario ha compromesso una AWS risorsa e l'ha alterata in modo che sia in grado di contattare il suo server di comando e controllo principale (C&C) per ricevere ulteriori istruzioni relative ad attività dannose.

Comportamento

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività diversi dalla linea di base stabilita per le risorse coinvolte. AWS

CredentialAccess

Questo valore indica che GuardDuty ha rilevato modelli di attività che un avversario può utilizzare per rubare credenziali, come password, nomi utente e chiavi di accesso, dall'ambiente dell'utente. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Criptovalute

Questo valore indica che GuardDuty è stato rilevato che una AWS risorsa nell'ambiente ospita software associato a criptovalute (ad esempio Bitcoin).

DefenseEvasion

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per evitare di essere rilevato mentre si infila nell'ambiente. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Individuazione

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per ampliare la propria conoscenza dei sistemi e delle reti interne. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Esecuzione

Questo valore indica che GuardDuty ha rilevato che un avversario potrebbe tentare di eseguire o ha già eseguito codice dannoso per esplorare l' AWS ambiente o rubare dati. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Esfiltrazione

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario può utilizzare per tentare di rubare dati dall'ambiente. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Impatto

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che suggeriscono che un avversario stia tentando di manipolare, interrompere o distruggere i sistemi e i dati. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

InitialAccess

Questo valore è comunemente associato alla fase di accesso iniziale di un attacco, quando un avversario tenta di stabilire l'accesso all'ambiente dell'utente. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Test di penetrazione (pen-test)

A volte i proprietari delle AWS risorse o i loro rappresentanti autorizzati eseguono intenzionalmente test sulle AWS applicazioni per individuare vulnerabilità, come gruppi di sicurezza aperti o chiavi di accesso eccessivamente permissive. Questi test di penetrazione vengono eseguiti nel tentativo di identificare e bloccare le risorse vulnerabili prima che siano individuate dagli avversari. Tuttavia, alcuni degli strumenti utilizzati dai tester autorizzati sono disponibili gratuitamente e quindi possono essere utilizzati da utenti non autorizzati o malintenzionati per eseguire test di probing. Sebbene non sia GuardDuty possibile identificare il vero scopo alla base di tale attività, il valore Pentest indica che GuardDuty è il rilevamento di tale attività, che è simile all'attività generata da noti strumenti di pen testing e che potrebbe indicare un sondaggio doloso della rete.

Persistence

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per cercare di mantenere l'accesso ai sistemi anche se la loro via di accesso iniziale è interrotta. Ad esempio, ciò potrebbe includere la creazione di un nuovo utente IAM dopo aver ottenuto l'accesso tramite le credenziali compromesse di un utente esistente. Quando le credenziali dell'utente esistente vengono eliminate, l'avversario manterrà l'accesso al nuovo utente che non è stato rilevato come parte dell'evento originale. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Policy

Questo valore indica che state mostrando Account AWS un comportamento contrario alle migliori pratiche di sicurezza consigliate. Ad esempio, la modifica involontaria delle politiche di autorizzazione associate alle AWS risorse o all'ambiente e l'uso di account privilegiati che dovrebbero avere un utilizzo minimo o nullo.

PrivilegeEscalation

Questo valore indica che il principale coinvolto nel tuo ambiente AWS ha un comportamento che un avversario potrebbe utilizzare per ottenere autorizzazioni di livello superiore per accedere alla rete. Questo scopo di minaccia si basa sulle [Tattiche MITRE ATT&CK](#).

Recon

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario può utilizzare per eseguire una ricognizione dell'ambiente per determinare come ampliare il proprio accesso o utilizzare le risorse dell'utente. Ad esempio, questa attività può includere l'individuazione delle vulnerabilità nell' AWS ambiente controllando le porte, effettuando chiamate API, elencando gli utenti ed elencando le tabelle del database, tra le altre cose.

Stealth

Questo valore indica che un avversario cerca attivamente di nascondere le proprie operazioni. Ad esempio, potrebbe utilizzare un server proxy anonimo, il che rende estremamente difficile valutare la vera natura dell'attività.

Trojan

Questo valore indica che un attacco utilizza programmi Trojan per svolgere attività dannose di nascosto. A volte questo software assume l'aspetto di un programma legittimo che gli utenti eseguono quindi involontariamente. In altre, questo software si esegue automaticamente sfruttando una vulnerabilità.

UnauthorizedAccess

Questo valore indica che GuardDuty sta rilevando un'attività sospetta o un modello di attività sospetto da parte di un individuo non autorizzato.

GuardDuty motore di scansione per il rilevamento di malware

Amazon GuardDuty dispone di un motore di scansione integrato e gestito internamente e di un [fornitore terzo](#). Entrambi utilizzano indicatori di compromissione (IoCs) provenienti da vari feed interni

che hanno visibilità sui diversi tipi di malware che potrebbero colpire. AWS GuardDuty include anche definizioni di rilevamento basate sulle regole YARA aggiunte dai nostri tecnici della sicurezza e rilevamenti basati su modelli euristici e di apprendimento automatico (ML). Durante la scansione di oggetti Amazon S3, GuardDuty Malware Protection produce risultati coerenti quando scansiona lo stesso oggetto più volte con le stesse definizioni e gli stessi motori di scansione. Il rilevamento basato sulla firma non include solo la corrispondenza dei byte, ma anche un frammento di codice potenzialmente complesso e lo scanner può analizzare i contenuti e prendere decisioni.

Il motore di scansione antimaleware non esegue analisi comportamentali in tempo reale, mentre la detonazione del malware monitora il campione mentre viene eseguito in un sistema reale. La GuardDuty soluzione è principalmente un rilevamento basato su file. Per rilevare malware senza file, GuardDuty fornisce una soluzione basata su agenti, ad esempio per [Monitoraggio del runtime](#) Amazon EKS, Amazon EC2 e Amazon ECS (incluso). AWS Fargate

Senza alcuna restrizione sui formati di file utilizzati per la scansione del malware, i motori di GuardDuty scansione che utilizza sono in grado di rilevare diversi tipi di malware, come cryptominer, ransomware e webshell. Il motore di GuardDuty scansione completamente gestito aggiorna continuamente l'elenco delle firme dei malware ogni 15 minuti.

Il motore di scansione fa parte del sistema di intelligence GuardDuty sulle minacce che utilizza un componente interno per la detonazione del malware. Ciò genera nuove informazioni sulle minacce raccogliendo in modo indipendente malware e campioni benigni da più fonti. Il tipo di file hash IoC del sistema di intelligence sulle minacce alimenta ulteriormente il motore di scansione antimaleware per rilevare il malware sulla base di hash di file dannosi noti.

Generazione di risultati campionari in GuardDuty

Amazon ti GuardDuty aiuta a generare risultati di esempio per visualizzare e comprendere i vari tipi di risultati che può generare. Quando generi risultati di esempio, GuardDuty compila l'elenco dei risultati attuali con un campione per ogni tipo di risultato supportato, compresi i tipi di rilevamento delle sequenze di attacco.

Gli esempi generati sono approssimazioni compilate con valori segnaposto. Questi esempi possono apparire diversi dai risultati reali relativi all'ambiente in uso, ma è possibile utilizzarli per testare varie configurazioni GuardDuty, ad esempio EventBridge eventi o filtri. Per un elenco dei valori disponibili per la ricerca dei tipi, consultate la [GuardDuty tipi di ricerca](#) tabella.

Generazione di risultati di esempio tramite la GuardDuty console o l'API

Scegli il metodo di accesso che preferisci per generare esiti di esempio.

Note

La GuardDuty console ti aiuta a generare un risultato per ogni tipo di risultato. Per generare uno o più tipi di risultati specifici, esegui i API/CLI passaggi associati.

Console

Utilizza la procedura seguente per generare esiti di esempio. Questo processo genera un risultato di esempio per ogni tipo di GuardDuty risultato.

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Settings (Impostazioni), in Sample findings (Risultati di esempio), selezionare Generate sample findings (Genera risultati di esempio).
4. Nel riquadro di navigazione, seleziona Esiti. Gli esiti di esempio vengono visualizzati nella pagina Risultati attuali con il prefisso [ESEMPIO].

API/CLI

È possibile generare un singolo risultato di esempio corrispondente a qualsiasi tipo di GuardDuty risultato tramite l'[CreateSampleFindings](#) API, i valori disponibili per la ricerca dei tipi sono elencati nella [GuardDuty tipi di ricerca](#) tabella.

Ciò è utile per testare le regole o l'automazione degli CloudWatch eventi in base ai risultati. L'esempio seguente mostra come generare un singolo esempio di esito del tipo `Backdoor:EC2/DenialofService.Tcp` utilizzando la AWS CLI.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/> console o esegui l'[ListDetectors](#) API.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--finding-types Backdoor:EC2/DenialofService.Tcp
```

Il titolo degli esiti di esempio generati con questi metodi inizia sempre con [ESEMPIO] nella console. Gli esiti di esempio hanno un valore di "sample": true nella sezione AdditionalInfo dei dettagli JSON degli esiti.

Per comprendere i dettagli dei risultati, ad esempio quelli relativi alla gravità e alla potenziale compromissione delle risorse, associati ai risultati generati, consulta [Livelli di gravità dei risultati GuardDuty](#) e [Dettagli degli esiti](#).

Per generare alcuni risultati comuni basati su un'attività simulata in un ambiente dedicato e isolato Account AWS all'interno del tuo ambiente, consulta. [GuardDuty Risultati dei test in account dedicati](#)

GuardDuty Risultati dei test in account dedicati

Usa questo documento per eseguire uno script di tester che generi GuardDuty risultati rispetto alle risorse di test che verranno distribuite nel tuo Account AWS. Puoi eseguire questi passaggi se desideri comprendere e conoscere determinati tipi di GuardDuty risultati e come i dettagli dei risultati si riferiscono alle risorse effettive del tuo account. Questa esperienza è diversa dalla generazione [Risultati di esempio](#). Per ulteriori informazioni sull'esperienza acquisita con GuardDuty i risultati dei test, vedere [Considerazioni](#).

Indice

- [Considerazioni](#)
- [GuardDuty lo script del tester dei risultati può generare](#)
- [Fase 1 - Prerequisiti](#)
- [Fase 2 - Implementazione delle risorse AWS](#)
- [Fase 3 - Esegui gli script dei tester](#)
- [Fase 4 - Pulisci le risorse di test AWS](#)
- [Risoluzione dei problemi comuni](#)

Considerazioni

Prima di procedere, tenete conto delle seguenti considerazioni:

- GuardDuty consiglia di utilizzare il tester in un ambiente non di produzione dedicato. Account AWS Questo approccio garantirà la capacità di identificare correttamente i GuardDuty risultati generati dal tester. Inoltre, il GuardDuty tester distribuisce una varietà di risorse che possono richiedere autorizzazioni IAM oltre a quelle consentite in altri account. L'utilizzo di un account dedicato

garantisce che le autorizzazioni possano essere assegnate correttamente con un limite di account chiaro.

- Lo script tester genera oltre 100 GuardDuty risultati con diverse combinazioni di risorse. AWS Attualmente, questo non include tutti i. [GuardDuty tipi di ricerca](#) Per un elenco dei tipi di ricerca che puoi generare con questo script di test, vedi. [GuardDuty lo script del tester dei risultati può generare](#)

Nota

Per visualizzare i tipi di ricerca delle sequenze di Attack, lo script tester genera solo e. [AttackSequence:EKS/CompromisedCluster](#) [AttackSequence:S3/CompromisedData](#) Per visualizzare e comprendere [AttackSequence:IAM/CompromisedCredentials](#), puoi generare [Risultati di esempio](#) nel tuo account.

- Affinché il GuardDuty tester funzioni come previsto, GuardDuty deve essere abilitato nell'account in cui vengono distribuite le risorse del tester. A seconda dei test che verranno eseguiti, il tester valuta se i piani di protezione GuardDuty appropriati sono abilitati o meno. Per qualsiasi piano di protezione non abilitato, GuardDuty richiederà l'autorizzazione per abilitare i piani di protezione necessari per un periodo sufficiente GuardDuty a eseguire i test che genereranno i risultati. Successivamente, GuardDuty disabiliterà il piano di protezione una volta completato il test.

Attivazione GuardDuty per la prima volta

Quando GuardDuty viene abilitato per la prima volta nel tuo account dedicato in una regione specifica, il tuo account verrà automaticamente registrato a una prova gratuita di 30 giorni.

GuardDuty offre piani di protezione opzionali. Al momento dell'attivazione GuardDuty, vengono attivati anche alcuni piani di protezione, inclusi nella prova gratuita di GuardDuty 30 giorni. Per ulteriori informazioni, consulta [Utilizzo GuardDuty della prova gratuita di 30 giorni](#).

GuardDuty è già abilitato nel tuo account prima di eseguire lo script tester

Se GuardDuty è già abilitato, in base ai parametri, lo script tester controllerà lo stato di configurazione di determinati piani di protezione e altre impostazioni a livello di account necessarie per generare i risultati.

Eseguendo questo script di test, alcuni piani di protezione potrebbero essere abilitati per la prima volta nell'account dedicato in una regione. Verrà così avviata la prova gratuita di 30 giorni per quel piano di protezione. Per informazioni sulla prova gratuita associata a ciascun piano di protezione, consulta [Utilizzo GuardDuty della prova gratuita di 30 giorni](#).

- Finché l'infrastruttura del GuardDuty tester è implementata, potresti ricevere occasionalmente dei [UnauthorizedAccess:EC2/TorClient](#) risultati dall' PenTest istanza.

GuardDuty lo script del tester dei risultati può generare

Attualmente, lo script tester genera i seguenti tipi di risultati relativi ai log di controllo di Amazon EC2, Amazon EKS, Amazon S3, IAM ed EKS:

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:S3/CompromisedData](#)
- [Backdoor:EC2/C&CAActivity.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](#)

Fase 1 - Prerequisiti

Per preparare l'ambiente di test, sono necessari i seguenti elementi:

- Git: installa lo strumento da riga di comando git in base al sistema operativo che utilizzi.

Questo è necessario per clonare il [amazon-guardduty-testerrepository](#).

- AWS Command Line Interface— Uno strumento open source che consente di interagire Servizi AWS utilizzando i comandi della shell della riga di comando. Per ulteriori informazioni, consulta la Guida [introduttiva AWS CLI nella Guida](#) per l'AWS Command Line Interface utente.
- AWS Systems Manager— Per avviare sessioni di Session Manager con i nodi gestiti utilizzando, AWS CLI è necessario installare il plug-in Session Manager sul computer locale. Per ulteriori informazioni, consulta [Installa il plug-in Session Manager AWS CLI nella Guida per](#) l'AWS Systems Manager utente.
- Node Package Manager (NPM): installa NPM per installare tutte le dipendenze.
- Docker: è necessario che Docker sia installato. Per istruzioni sull'installazione, consulta il [sito Web Docker](#).

Per verificare che Docker sia stato installato, esegui il comando seguente e conferma che esista un output simile al seguente:

```
$ docker --version
```

```
Docker version 19.03.1
```

- Iscriviti all'immagine di [Kali Linux](#) in. Marketplace AWS

Fase 2 - Implementazione delle risorse AWS

Questa sezione fornisce un elenco di concetti chiave e i passaggi per distribuire determinate AWS risorse nel tuo account dedicato.

Concetti

L'elenco seguente fornisce i concetti chiave relativi ai comandi che consentono di distribuire le risorse:

- AWS Cloud Development Kit (AWS CDK)— CDK è un framework di sviluppo software open source per definire l'infrastruttura cloud in codice e fornirla tramite. CloudFormation CDK supporta un paio di linguaggi di programmazione per definire componenti cloud riutilizzabili noti come costrutti. Puoi comporli insieme in pile e app. Quindi, puoi distribuire le tue applicazioni CDK per effettuare il provisioning o CloudFormation aggiornare le tue risorse. Per ulteriori informazioni, consulta [Cos'è il? AWS CDK](#) nella Guida per gli AWS Cloud Development Kit (AWS CDK) sviluppatori.
- Bootstrap: è il processo di preparazione dell' AWS ambiente per l'utilizzo con. AWS CDK Prima di implementare uno stack CDK in un AWS ambiente, è necessario avviare l'ambiente. Questo processo di approvvigionamento di AWS risorse specifiche nell'ambiente utilizzate da AWS CDK fa parte dei passaggi che verranno eseguiti nella prossima sezione -. [Passaggi per distribuire le risorse AWS](#)

Per ulteriori informazioni su come funziona il bootstrap, consulta Bootstrapping nella [Developer Guide](#).AWS Cloud Development Kit (AWS CDK)

Passaggi per distribuire le risorse AWS

Esegui i passaggi seguenti per iniziare a distribuire le risorse:

1. Configura l'account e la regione AWS CLI predefiniti, a meno che le variabili Region dell'account dedicato non vengano impostate manualmente nel `bin/cdk-gd-tester.ts` file. Per ulteriori informazioni, consulta [Environments](#) nella AWS Cloud Development Kit (AWS CDK) Developer Guide.
2. Esegui i seguenti comandi per distribuire le risorse:

```
git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

L'ultimo comando (`cdk deploy`) crea uno CloudFormation stack per tuo conto. Il nome di questo stack è. `GuardDutyTesterStack`

Come parte di questo script, GuardDuty crea nuove risorse per generare GuardDuty risultati nel tuo account. Aggiunge inoltre la seguente coppia di tag `key:value` alle istanze Amazon EC2:

`CreatedBy:GuardDuty Test Script`

Le istanze Amazon EC2 includono anche le istanze EC2 che ospitano nodi EKS e cluster ECS.

Tipi di istanza

GuardDuty è progettato per utilizzare tipi di istanze convenienti che forniscono le prestazioni minime necessarie per eseguire correttamente i test. A causa dei requisiti vCPU, il gruppo di nodi Amazon EKS richiede `et3.medium`, a causa della maggiore capacità di rete richiesta per la DenialOfService ricerca dei test, il nodo driver richiede. `m6i.large` Per tutti gli altri test, GuardDuty utilizza il tipo di `t3.micro` istanza. Per ulteriori informazioni sui tipi di istanze, consulta [le dimensioni disponibili](#) nella Amazon EC2 Instances Types Guide.

Fase 3 - Esegui gli script dei tester

Si tratta di un processo in due fasi in cui è necessario prima avviare una sessione con il test driver e quindi eseguire script per generare GuardDuty risultati con combinazioni di risorse specifiche.

Parte A - Inizia la sessione con il test driver

1. Dopo aver distribuito le risorse, salvate il codice regionale in una variabile nella sessione di terminale corrente. Utilizzate il comando seguente e `us-east-1` sostituitelo con il codice regionale in cui avete distribuito le risorse:

```
$ REGION=us-east-1
```

2. Lo script tester è disponibile solo tramite AWS Systems Manager (SSM). Per avviare una shell interattiva sull'istanza dell'host del tester, interroga l'host. InstanceId
3. Utilizzate il seguente comando per iniziare la sessione per lo script tester:

```
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)
```

Parte B - Generazione di risultati

Lo script tester è un programma basato su Python che crea dinamicamente uno script bash per generare risultati in base al tuo input. Hai la flessibilità necessaria per generare risultati basati su uno o più tipi di AWS risorse, piani di GuardDuty protezione, (tattiche) o. [Scopi delle minacce](#) [Origini dati fondamentali](#) [the section called “GuardDuty lo script del tester dei risultati può generare”](#)

Utilizza i seguenti esempi di comandi come riferimento ed esegui uno o più comandi per generare risultati da esplorare:

```
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'
```

Per ulteriori informazioni sui parametri validi, puoi eseguire il seguente comando help:

```
python3 guardduty_tester.py --help
```

Parte C - Esamina i risultati generati

Scegli un metodo preferito per visualizzare i risultati generati nel tuo account.

GuardDuty console

1. Accedi Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, seleziona Esiti.
3. Dalla tabella dei risultati, seleziona un risultato di cui desideri visualizzare i dettagli. Si aprirà il pannello dei dettagli del risultato. Per informazioni, consulta [Comprendere e generare i GuardDuty risultati di Amazon](#).
4. Se desideri filtrare questi risultati, usa la chiave e il valore del tag di risorsa. Ad esempio, per filtrare i risultati generati per le istanze Amazon EC2, utilizza **CreatedBy: GuardDuty Test Script** tag key:value pair for Instance tag key e Instance tag key.

API

- Esegui [ListFindings](#) per visualizzare i risultati relativi a uno specifico ID del rilevatore. È possibile filtrare i risultati con parametri specifici.

Per trovare i detectorId dati relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

AWS CLI

- Esegui il AWS CLI comando seguente per visualizzare i risultati generati *us-east-1* e sostituirli *12abc34d567e8fa901bc2d34EXAMPLE* con i valori appropriati:

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```

Per trovare le detectorId impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Per ulteriori informazioni sui parametri che puoi utilizzare per filtrare i risultati, consulta [list-finding](#) nel AWS CLI Command Reference.

Fase 4 - Pulisci le risorse di test AWS

Le impostazioni a livello di account e gli altri aggiornamenti dello stato di configurazione effettuati [Fase 3 - Esegui gli script dei tester](#) tornano allo stato originale al termine dello script del tester.

Dopo aver eseguito lo script del tester, puoi scegliere di ripulire le risorse del test. AWS Puoi scegliere di eseguire questa operazione utilizzando uno dei seguenti metodi:

- Esegui il comando seguente:

```
cdk destroy
```

- Eliminare lo CloudFormation stack con il nome GuardDutyTesterStack. Per informazioni sui passaggi, vedi [Eliminazione di uno stack sulla console](#). CloudFormation

Risoluzione dei problemi comuni

GuardDuty ha identificato problemi comuni e consiglia le procedure per la risoluzione dei problemi:

- Cloud assembly schema version mismatch— Aggiorna la AWS CDK CLI a una versione compatibile con la versione di cloud assembly richiesta o all'ultima versione disponibile. Per ulteriori informazioni, consulta [AWS CDK Compatibilità CLI](#).
- Docker permission denied— Aggiungi l'utente dell'account dedicato al docker o agli utenti docker in modo che l'account dedicato possa eseguire i comandi. [Per ulteriori informazioni sui passaggi, consulta l'opzione Daemon socket](#).
- Your requested instance type is not supported in your requested Availability Zone— Alcune zone di disponibilità non supportano particolari tipi di istanze. Per identificare quali zone di disponibilità supportano il tipo di istanza preferito e tentare nuovamente di distribuire AWS le risorse, procedi nel seguente modo:
 1. Scegli un metodo preferito per determinare quali zone di disponibilità supportano il tuo tipo di istanza:

Console

Per identificare le zone di disponibilità che supportano il tipo di istanza preferito

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/>
2. Utilizzando il selettore AWS della regione nell'angolo in alto a destra della pagina, scegli la regione in cui desideri avviare l'istanza.
3. Nel riquadro di navigazione, in Istanze, scegli Tipi di istanze.
4. Dalla tabella Tipi di istanze, scegli un tipo di istanza preferito.
5. In Rete, visualizza le regioni elencate in Zone di disponibilità.

In base a queste informazioni, potrebbe essere necessario scegliere una nuova regione in cui distribuire le risorse.

AWS CLI

Esegui il comando seguente per visualizzare un elenco di zone di disponibilità. Assicurati di specificare il tipo di istanza preferito e la regione (*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
```

Per ulteriori informazioni su questo comando, [describe-instance-type-offerings](#) consultate la sezione AWS CLI Command Reference.

Quando esegui questo comando, se ricevi un errore, assicurati di utilizzare la versione più recente di AWS CLI. Per ulteriori informazioni, consulta la sezione [Risoluzione dei problemi](#) nella Guida per l'utente di AWS Command Line Interface .

2. Prova a distribuire nuovamente le AWS risorse e specifica una zona di disponibilità che supporti il tipo di istanza preferito.

Per riprovare a distribuire le risorse AWS

1. Imposta la regione predefinita nel file. `bin/cdk-gd-tester.ts`

2. Per specificare la zona di disponibilità, apri il `amazon-guardduty-tester/lib/common/network/vpc.ts` file.
3. In questo file, `maxAzs: 2`, sostituisilo con `availabilityZones: ['us-east-1a', 'us-east-1c']`, dove devi specificare le zone di disponibilità per il tipo di istanza.
4. Continua con i passaggi rimanenti riportati di seguito [Passaggi per distribuire le risorse AWS](#).

Visualizzazione dei risultati generati nella console GuardDuty

Quando GuardDuty rileva un'attività che corrisponde al modello di un problema di sicurezza, GuardDuty genera un risultato. Questo risultato è associato a un tipo di risorsa che potrebbe essere stata compromessa durante questa attività. È possibile visualizzare i dettagli associati a ogni risultato GuardDuty generato.

Se si utilizza un account GuardDuty amministratore, è possibile visualizzare i risultati generati per conto degli account dei membri. Tuttavia, un account membro può visualizzare i risultati generati nel proprio account. Un account membro non può visualizzare i risultati generati per gli account di altri membri.

Procedura per visualizzare i risultati nella GuardDuty console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione a sinistra, scegli Findings.

GuardDuty visualizza i risultati in formato tabulare. Per impostazione predefinita, questa tabella è ordinata in ordine decrescente in base al valore dell'ultima colonna visualizzata, con i risultati più recenti nella parte superiore.

I risultati con l'icona a forma di spada



rappresentano un risultato della sequenza di attacco.

3. Per visualizzare i dettagli associati a un risultato, selezionane il titolo. Si aprirà il pannello laterale con i dettagli del risultato. Per trovare la sequenza di attacco, questo pannello laterale include una versione riassuntiva della sequenza di attacco; per espandere questa visualizzazione, scegli Visualizza dettagli.

Per informazioni sui campi elencati in questo pannello laterale, consulta [Dettagli degli esiti](#).

4. (Facoltativo) per scaricare Finding JSON

- a. Seleziona il risultato, quindi scegli il menu Azioni.
- b. Nel menu Azioni, scegli Visualizza ed esporta JSON.
- c. Nella finestra Findings JSON, scegli Scarica.

Note

In alcuni casi, GuardDuty si rende conto che alcuni risultati sono falsi positivi dopo che sono stati generati. GuardDuty fornisce un campo Confidence nel codice JSON del risultato e ne imposta il valore su zero. In questo modo GuardDuty saprai che puoi tranquillamente ignorare tali risultati.

I risultati senza il campo Confidenza non sono considerati falsi positivi.

Navigazione nella pagina dei risultati

Questa sezione fornisce informazioni chiave sui vari elementi della pagina Risultati. Questo ti aiuterà ad analizzare i risultati generati per l'analisi e la risposta alle minacce.

L'elenco seguente illustra gli elementi della pagina Risultati che consentono di comprendere meglio i risultati generati:

- Tipo di minaccia:

Il tipo di minaccia include GuardDuty i risultati individuali e i risultati della sequenza di attacco. Per impostazione predefinita, la pagina mostra Tutti i risultati.

Per filtrare la visualizzazione della tabella dei risultati, nel menu Tipo di minaccia, scegli una delle opzioni: Solo risultati della sequenza di attacco o Solo risultati individuali.

- Colonne Resource e Count:

La colonna Risorsa nella tabella dei risultati mostra il nome della AWS risorsa potenzialmente compromessa. Per determinare la sequenza di attacco, questa colonna mostra il numero di risorse potenzialmente compromesse AWS. Per visualizzare i nomi delle risorse, selezionate il numero nella colonna Risorsa.

La colonna Count indica il numero di volte in cui viene GuardDuty osservato un risultato specifico. Quando GuardDuty rileva che un'attività corrisponde a un problema di sicurezza identificato in

precedenza, incrementa il conteggio per quel risultato specifico. Per il rilevamento della sequenza di attacco, questo valore di colonna indica il numero totale di segnali e risultati coinvolti nella generazione del risultato.

- Ordinamento dei risultati per colonne della tabella:

Se c'è una freccia accanto all'intestazione di una colonna, puoi ordinare la tabella dei risultati in base alla colonna. Seleziona l'intestazione della colonna per ordinare i risultati in ordine crescente o decrescente del valore in quella colonna.

- Filtraggio dei risultati:

In base a specifici attributi di proprietà, ad esempio Account ID e Resource type, è possibile filtrare ulteriormente la tabella dei risultati. Per informazioni sui tipi di filtri che è possibile utilizzare, vedere [Filtraggio GuardDuty dei risultati](#).

- Status e regole salvate:

Il menu Stato include due valori: Corrente e Archiviato. La visualizzazione predefinita è Risultati correnti nella tabella.

Quando non desideri più GuardDuty generare un risultato che corrisponda a un criterio specifico, puoi sopprimerlo. GuardDuty archivia tale risultato. Quando GuardDuty rileva nuovamente questo risultato, non riceverai alcuna notifica di questa osservazione. Per visualizzare in modo specifico i risultati archiviati, nel menu Stato, scegli Archiviato.

Le regole salvate sono una funzionalità che consente di filtrare automaticamente e intraprendere azioni sui risultati che corrispondono a criteri specifici. Le azioni possono includere l'archiviazione dei risultati o la loro soppressione dalle notifiche future.

Per ulteriori informazioni, consulta [Regole di eliminazione](#).

Livelli di gravità dei risultati GuardDuty

A ogni GuardDuty risultato è assegnato un livello di gravità e un valore che riflettono il rischio potenziale che il risultato potrebbe comportare per l'ambiente dell'utente, secondo quanto stabilito dai nostri tecnici della sicurezza. Il valore della gravità può rientrare in un intervallo compreso tra 1,0 e 10,0, mentre valori più alti indicano un rischio maggiore per la sicurezza. Per aiutarti a determinare una risposta a un potenziale problema di sicurezza evidenziato da un risultato, GuardDuty suddivide questo intervallo in livelli di gravità critico, alto, medio e basso.

Un risultato di un tipo particolare può avere una gravità diversa a seconda del contesto specifico del risultato. Per visualizzare un elenco consolidato dei livelli di gravità predefiniti per tutti i tipi GuardDuty di risultati, vedere [GuardDuty tipi di ricerca attivi](#).

Le sezioni seguenti spiegano i livelli di gravità definiti per i GuardDuty risultati.

Argomenti

- [Gravità critica](#)
- [Severità elevata](#)
- [Gravità media](#)
- [Bassa severità](#)

Gravità critica

Intervallo di valori: 9,0 - 10,0

Descrizione: un livello di gravità critico indica che una sequenza di attacco potrebbe essere in corso o essere avvenuta di recente. Una o più AWS risorse, come le credenziali di accesso degli utenti IAM e il bucket Amazon S3, sono potenzialmente compromesse o potrebbero essere già state compromesse.

Raccomandazione: GuardDuty consiglia di dare priorità alla valutazione e alla correzione di tutte le rilevazioni di gravità critica, poiché questi problemi possono far parte di un attacco ransomware e possono aggravarsi in qualsiasi momento. Visualizza i dettagli sulle risorse coinvolte e inizia a risolvere i problemi di sicurezza. Per ulteriori informazioni, consulta [Correzioni degli esiti](#).

Severità elevata

Intervallo di valori: 7,0 - 8,9

Descrizione: un livello di severità elevato indica che la risorsa in questione (un'istanza Amazon EC2 o un set di credenziali di accesso utente IAM) è compromessa e viene utilizzata attivamente per scopi non autorizzati.

Raccomandazione: GuardDuty consiglia di considerare prioritario qualsiasi problema di sicurezza di rilevazione di elevata gravità e di adottare misure correttive immediate per prevenire un ulteriore utilizzo non autorizzato delle risorse. Ad esempio, pulisci l'istanza Amazon EC2 o terminala o ruota le credenziali IAM. Segui i passaggi indicati per correggere il risultato [Correzioni degli esiti](#).

Gravità media

Intervallo di valori: 4,0 - 6,9

Descrizione: un livello di gravità medio indica un'attività sospetta che si discosta dal comportamento normalmente osservato e, a seconda del caso d'uso, può essere indicativa di una compromissione delle risorse.

Raccomandazione: GuardDuty consiglia di esaminare la risorsa potenzialmente interessata il prima possibile. Le fasi di riparazione varieranno in base alla risorsa e alla ricerca di una famiglia. Un approccio consolidato consiste nel confermare che l'attività è autorizzata e coerente con il caso d'uso. Se non riesci a identificare la causa o a confermare che l'attività è stata autorizzata, dovresti considerare la risorsa compromessa. Segui i passaggi indicati [Correzioni degli esiti](#) per correggere il problema.

Ecco alcuni aspetti da considerare quando si esamina un risultato di medio livello:

- Controlla se un utente autorizzato ha installato un nuovo software che ha modificato il comportamento di una risorsa (ad esempio, consentito un traffico da alto a normale o abilitato le comunicazioni su una nuova porta).
- Controlla se un utente autorizzato ha modificato le impostazioni del piano di controllo, ad esempio ha modificato un'impostazione del gruppo di sicurezza.
- Esegui una scansione antivirus sulla risorsa coinvolta per rilevare il software non autorizzato.
- Verifica le autorizzazioni collegate a ruolo, utente, gruppi o un set di credenziali IAM coinvolti. Queste potrebbero essere modificate o ruotate.

Bassa severità

Intervallo di valori: 1,0 - 3,9

Descrizione: un livello di gravità basso indica un tentativo di attività sospetta che non ha compromesso l'ambiente, ad esempio una scansione delle porte o un tentativo di intrusione fallito.

Raccomandazione: non esiste un'azione immediata consigliata, ma vale la pena prendere nota di queste informazioni in quanto potrebbero indicare che qualcuno sta cercando punti deboli nell'ambiente in uso.

Dettagli degli esiti

Nella GuardDuty console Amazon, puoi visualizzare i dettagli della ricerca nella sezione di riepilogo dei risultati. I dettagli degli esiti variano in base al tipo di esito.

Esistono due dettagli principali che determinano il tipo di informazioni disponibili per qualsiasi esito. Il primo è il tipo di risorsa, che può essere `Instance AccessKeyS3Bucket`, `S3Object`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance`, `RDSLimitlessDB`, `oLambda`. Il secondo dettaglio che determina le informazioni sull'esito è Ruolo risorsa. Il ruolo della risorsa può essere `Target`, il che significa che la risorsa è stata oggetto di attività sospette. Per gli esiti del tipo istanza, il ruolo risorsa può anche essere `Actor`, che indica che la risorsa è stata l'attore che svolgeva attività sospette. In questo argomento vengono descritti alcuni dei dettagli degli esiti comunemente disponibili. Per [the section called “Tipi di risultati del monitoraggio del runtime”](#) e [Protezione da malware per tipo di ricerca S3](#), il ruolo della risorsa non è popolato.

Argomenti

- [Panoramica degli esiti](#)
- [Risorsa](#)
- [Dettagli sulla ricerca della sequenza di attacco](#)
- [Dettagli utente del database \(DB\) RDS](#)
- [Dettagli sugli esiti del monitoraggio del runtime](#)
- [Dettagli della scansione dei volumi EBS](#)
- [Dettagli sulla ricerca di Malware Protection for EC2](#)
- [Dettagli sugli esiti di Malware Protection per S3](#)
- [Azione](#)
- [Attore o destinazione](#)
- [Dettagli sulla geolocalizzazione](#)
- [Informazioni aggiuntive](#)
- [Evidenza](#)
- [Comportamento anomalo](#)

Panoramica degli esiti

La sezione Panoramica di un esito ne contiene le caratteristiche identificative di base, incluse le informazioni seguenti:

- ID account: l'ID dell' AWS account in cui si è svolta l'attività che ha richiesto la generazione GuardDuty di questo risultato.
- Conteggio: il numero di volte in cui GuardDuty è stata aggregata un'attività che corrisponde a questo schema a questo risultato ID.
- Ora creazione: la data e l'ora di creazione di questo esito. Se questo valore è diverso da Ora aggiornamento significa che l'attività si è verificata più volte e si tratta di un problema in corso.

Note

I timestamp per i risultati nella GuardDuty console vengono visualizzati nel fuso orario locale, mentre le esportazioni JSON e gli output CLI visualizzano i timestamp in UTC.

- ID risultato: un identificatore univoco per questo tipo di esito e insieme di parametri. Le nuove occorrenze di attività corrispondenti a questo modello verranno aggregate allo stesso ID.
- Tipo di esito: una stringa formattata che rappresenta il tipo di attività che ha attivato l'esito. Per ulteriori informazioni, consulta [GuardDuty formato di ricerca](#).
- Regione: la regione in cui è stato generato il risultato. AWS Per ulteriori informazioni sulle regioni supportate, consulta [Regioni ed endpoint](#).
- ID risorsa: l'ID della AWS risorsa in base alla quale si è svolta l'attività che ha portato GuardDuty alla generazione del risultato.
- ID di scansione: applicabile ai risultati quando GuardDuty Malware Protection for EC2 è abilitata, si tratta di un identificatore della scansione antimalware eseguita sui volumi EBS collegati al carico di lavoro dell'istanza o del contenitore EC2 potenzialmente compromesso. Per ulteriori informazioni, consulta [Dettagli sulla ricerca di Malware Protection for EC2](#).
- Severità: a un risultato viene assegnato un livello di gravità che può essere Critico, Alto, Medio o Basso. Per ulteriori informazioni, consulta [Livelli di gravità dei risultati](#).
- Aggiornato il: l'ultima volta che questo risultato è stato aggiornato con una nuova attività corrispondente allo schema che ha portato GuardDuty alla generazione di questo risultato.

Risorsa

La risorsa interessata fornisce dettagli sulla AWS risorsa presa di mira dall'attività iniziale. Le informazioni disponibili variano in base al tipo di risorsa e al tipo di operazione.

Ruolo della risorsa: il ruolo della AWS risorsa che ha avviato la ricerca. Questo valore può essere TARGET o ACTOR e indica se la risorsa era la destinazione dell'attività sospetta o l'attore che l'ha messa in atto.

Tipo di risorsa: il tipo di risorsa interessata. Un esito può includere diversi tipi di risorse se sono state coinvolte più risorse. I tipi di risorse sono Instance AccessKey, S3Bucket, S3Object,,, Container KubernetesClusterECSCluster, RDSDBInstanceDB RDSLimitless e Lambda. A seconda del tipo di risorsa sono disponibili diversi dettagli degli esiti. Seleziona una scheda delle opzioni di risorsa per scoprire i dettagli disponibili per la risorsa interessata.

Instance

Dettagli dell'istanza:

Note

Potrebbero mancare alcuni dettagli se l'istanza è già stata interrotta o se l'invocazione dell'API sottostante ha avuto origine da un'istanza EC2 in una regione durante una chiamata API tra regioni.

- ID istanza: l'ID dell'istanza EC2 coinvolta nell'attività che ha portato alla generazione del risultato. GuardDuty
- Tipo di istanza: il tipo dell'istanza EC2 coinvolta nell'esito.
- Ora di avvio: la data e l'ora in cui l'istanza è stata avviata.
- Outpost ARN — L'Amazon Resource Name (ARN) di. AWS Outposts Applicabile solo alle istanze. AWS Outposts Per ulteriori informazioni, consulta [Cos'è AWS Outposts?](#) nella Guida per l'utente degli scaffali Outposts.
- Nome del gruppo di sicurezza: il nome del gruppo di sicurezza collegato all'istanza interessata.
- ID gruppo di sicurezza: l'ID del gruppo di sicurezza collegato all'istanza interessata.
- Stato dell'istanza: lo stato attuale dell'istanza di destinazione.

- Zona di disponibilità: la zona di disponibilità della regione AWS in cui si trova l'istanza coinvolta.
- ID immagine: l'ID dell'Amazon Machine Image utilizzato per creare l'istanza coinvolta nell'attività.
- Descrizione immagine: una descrizione dell'ID dell'Amazon Machine Image utilizzato per creare l'istanza coinvolta nell'attività.
- Tag: un elenco di tag collegati a questa risorsa elencati nel formato key:value.

AccessKey

Dettagli chiave di accesso:

- ID chiave di accesso: l'ID della chiave di accesso dell'utente impegnato nell'attività che ha portato GuardDuty alla generazione del risultato.
- ID principale: l'ID principale dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Tipo di utente: il tipo di utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato. Per ulteriori informazioni, consulta [Elemento userIdentity di CloudTrail](#).
- Nome utente: il nome dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.

S3Bucket

Dettagli bucket Amazon S3:

- Nome: il nome del bucket coinvolto nell'esito.
- ARN: l'ARN del bucket coinvolto nell'esito.
- Proprietario: l'ID utente canonico dell'utente proprietario del bucket coinvolto nell'esito. [Per ulteriori informazioni sugli utenti canonici, IDs consulta AWS gli identificatori dell'account.](#)
- Tipo: il tipo di esito del bucket può essere Destinazione o Origine.
- Crittografia lato server predefinita: i dettagli di crittografia per il bucket.
- Tag bucket: un elenco dei tag collegati a questa risorsa, elencati nel formato di key:value.
- Autorizzazioni valide: una valutazione di tutte le autorizzazioni e le policy valide nel bucket che indica se il bucket interessato è esposto pubblicamente. I valori possono essere Pubblico o Non pubblico.

S3Object

- Dettagli dell'oggetto S3: include le seguenti informazioni sull'oggetto S3 scansionato:
 - ARN — Amazon Resource Name (ARN) dell'oggetto S3 scansionato.
 - Chiave: il nome assegnato al file quando è stato creato nel bucket S3.
 - ID versione: se hai abilitato il controllo delle versioni del bucket, questo campo indica l'ID della versione associato all'ultima versione dell'oggetto S3 scansionato. Per ulteriori informazioni, consulta [Using versioning in bucket S3](#) nella Amazon S3 User Guide.
 - ETag: rappresenta la versione specifica dell'oggetto S3 scansionato.
 - Hash: hash della minaccia rilevata in questo risultato.
- Dettagli sul bucket S3: include le seguenti informazioni sul bucket Amazon S3 associato all'oggetto S3 scansionato:
 - Nome: indica il nome del bucket S3 che contiene l'oggetto.
 - ARN — Amazon Resource Name (ARN) del bucket S3.
- Proprietario: ID canonico del proprietario del bucket S3.

EKSCluster

Dettagli del cluster Kubernetes:

- Nome: il nome del cluster Kubernetes.
- ARN: l'ARN che identifica il cluster.
- Ora creazione: la data e l'ora di creazione di questo cluster.

Note

I timestamp per i risultati nella GuardDuty console vengono visualizzati nel fuso orario locale, mentre le esportazioni JSON e gli output CLI visualizzano i timestamp in UTC.

- ID VPC: l'ID del VPC associato al cluster.
- Stato: lo stato attuale del cluster.
- Tag: i metadati applicati al cluster utili per catalogarli e organizzarli. Ciascun tag è formato da una chiave e da un valore facoltativo, elencati nel formato `key:value`. Puoi definire sia la chiave che il valore.

I tag del cluster non si propagano ad altre risorse associate al cluster.

Dettagli del carico di lavoro Kubernetes:

- Tipo: il tipo di carico di lavoro Kubernetes, ad esempio pod, implementazione e processo.
- Nome: il nome del carico di lavoro Kubernetes.
- Uid: l'ID univoco del carico di lavoro Kubernetes.
- Ora creazione: la data e l'ora di creazione di questo carico di lavoro.
- Etichette: le coppie chiave-valore collegate al carico di lavoro Kubernetes.
- Container: i dettagli del container in esecuzione come parte del carico di lavoro Kubernetes.
- Spazio dei nomi: il carico di lavoro appartiene a questo spazio dei nomi Kubernetes.
- Volumi: i volumi utilizzati dal carico di lavoro Kubernetes.
 - Percorso host: rappresenta un file o una directory preesistente sulla macchina host a cui è mappato il volume.
 - Nome: il nome del volume.
- Contesto di sicurezza del pod: definisce i privilegi e le impostazioni di controllo degli accessi per tutti i container in un pod.
- Rete host: impostata su `true` se i pod sono inclusi nel carico di lavoro Kubernetes.

Dettagli utente Kubernetes:

- Gruppi: gruppi Kubernetes RBAC (controllo degli accessi basato sul ruolo) dell'utente coinvolto nell'attività che ha generato l'esito.
- ID: l'ID univoco dell'utente Kubernetes.
- Nome utente: nome dell'utente Kubernetes coinvolto nell'attività che ha generato l'esito.
- Nome sessione: entità che ha assunto il ruolo IAM con le autorizzazioni RBAC di Kubernetes.

ECSCluster

Dettagli del cluster ECS:

- ARN: l'ARN che identifica il cluster.
- Nome: il nome del cluster.

- Stato: lo stato attuale del cluster.
- Numero di servizi attivi: il numero dei servizi in esecuzione sul cluster con stato ACTIVE. Puoi visualizzare questi servizi con [ListServices](#)
- Numero di istanze di container registrate: il numero delle istanze di container registrate nel cluster, incluse sia le istanze di container con stato ACTIVE che quelle con stato DRAINING.
- Numero di attività in esecuzione: il numero di attività con stato RUNNING nel cluster.
- Tag: i metadati applicati al cluster utili per catalogarli e organizzarli. Ciascun tag è formato da una chiave e da un valore facoltativo, elencati nel formato key:value. Puoi definire sia la chiave che il valore.
- Container: i dettagli sul container associato all'attività.
 - Nome container: il nome del container.
 - Immagine del container: l'immagine del container.
- Dettagli dell'attività: i dettagli di un'attività in un cluster.
 - ARN: il nome della risorsa Amazon (ARN) dell'attività.
 - ARN di definizione: il nome della risorsa Amazon (ARN) della definizione dell'attività che crea l'attività.
 - Versione: il contatore delle versioni per l'attività.
 - Ora creazione attività: il timestamp Unix al momento della creazione dell'attività.
 - Ora inizio attività: il timestamp Unix all'inizio dell'attività.
 - Attività iniziata da: il tag specificato all'avvio di un'attività.

Container

Dettagli container:

- Runtime del container: il runtime del container (ad esempio docker o containerd) utilizzato per eseguire il container.
- ID: l'ID dell'istanza di container o le voci ARN complete per l'istanza di container.
- Nome: il nome del container.
- Immagine: l'immagine dell'istanza di container.
- Montaggi volume: elenco dei montaggi del volume del container. Un container può montare un volume nel proprio file system.

- **Contesto di sicurezza:** il contesto di sicurezza del container definisce i privilegi e le impostazioni di controllo degli accessi per un container.
- **Dettagli del processo:** descrive i dettagli del processo associato all'esito.

RDSDBInstance

RDSDBInstance dettagli:

Note

Questa risorsa è disponibile negli esiti della Protezione RDS relativi all'istanza di database.

- **ID dell'istanza del database:** l'identificatore associato all'istanza di database coinvolta nel GuardDuty risultato.
- **Motore:** il nome del motore di database dell'istanza di database coinvolta nell'esito. I valori possibili sono compatibili con Aurora MySQL o Aurora PostgreSQL.
- **Versione del motore:** la versione del motore di database coinvolta nel GuardDuty risultato.
- **ID del cluster di database:** l'identificatore del cluster di database che contiene l'ID dell'istanza di database coinvolta nel GuardDuty risultato.
- **ARN dell'istanza di database:** l'ARN che identifica l'istanza di database coinvolta nel risultato. GuardDuty

RDSLimitlessDB

RDSLimitlessDettagli del database:

Questa risorsa è disponibile nei risultati di RDS Protection relativi alla versione del motore supportata di Limitless Database.

- **Identificatore del gruppo di shard DB:** il nome associato al gruppo di shard DB Limitless.
- **ID di risorsa del gruppo di shard DB:** l'identificatore di risorsa del gruppo di shard DB all'interno del DB Limitless.
- **ARN del gruppo di shard DB:** Amazon Resource Name (ARN) che identifica il gruppo di shard DB.
- **Motore:** l'identificatore del DB Limitless coinvolto nella scoperta.

- Versione del motore: la versione del motore Limitless DB.
- Identificatore del cluster DB: il nome del cluster di database che fa parte del DB Limitless.

Per informazioni sui dettagli relativi all'utente e all'autenticazione del database potenzialmente interessato, vedere. [Dettagli utente del database \(DB\) RDS](#)

Lambda

Dettagli della funzione Lambda

- Nome funzione: il nome della funzione Lambda coinvolta nell'esito.
- Versione della funzione: la versione della funzione Lambda coinvolta nell'esito.
- Descrizione della funzione: una descrizione della funzione Lambda coinvolta nell'esito.
- Funzione ARN: il nome della risorsa Amazon (ARN) della funzione Lambda coinvolta nell'esito.
- ID revisione: l'ID di revisione della versione della funzione Lambda.
- Ruolo: il ruolo di esecuzione della funzione Lambda coinvolta nell'esito.
- Configurazione VPC: la configurazione Amazon VPC, che include l'ID VPC, il gruppo di sicurezza e la sottorete associati alla funzione Lambda. IDs
 - ID VPC: l'ID dell'Amazon VPC associato alla funzione Lambda coinvolta nell'esito.
 - Subnet IDs: l'ID delle sottoreti associate alla funzione Lambda.
 - Gruppo di sicurezza: il gruppo di sicurezza collegato alla funzione Lambda coinvolta. Sono inclusi il nome e l'ID del gruppo di sicurezza.
- Tag: un elenco di tag collegati a questa risorsa, elencati nel formato della coppia key:value.

Dettagli sulla ricerca della sequenza di attacco

GuardDuty fornisce dettagli per ogni risultato generato nel tuo account. Questi dettagli ti aiutano a comprendere i motivi alla base della scoperta. Questa sezione si concentra sui dettagli associati [ai tipi di ricerca delle sequenze di attacco](#). Ciò include informazioni quali le risorse potenzialmente interessate, la cronologia degli eventi, gli indicatori, i segnali e gli endpoint coinvolti nella scoperta.

Per visualizzare i dettagli associati ai segnali considerati GuardDuty risultati, consulta le sezioni associate in questa pagina.

Nella GuardDuty console, quando selezioni la ricerca di una sequenza di attacco, il pannello laterale dei dettagli è suddiviso nelle seguenti schede:

- **Panoramica:** fornisce una visione compatta dei dettagli della sequenza di attacco, inclusi segnali, tattiche MITRE e risorse potenzialmente interessate.
- **Segnali:** visualizza una sequenza temporale degli eventi coinvolti in una sequenza di attacco.
- **Risorse:** fornisce informazioni sulle risorse potenzialmente interessate o sulle risorse potenzialmente a rischio.

L'elenco seguente fornisce le descrizioni associate ai dettagli di ricerca della sequenza di attacco.

Segnali

Un segnale potrebbe essere un'attività API o un risultato GuardDuty utilizzato per rilevare una sequenza di attacco. GuardDuty considera i segnali deboli che non si presentano come una minaccia evidente, li mette insieme e li mette in correlazione con i risultati generati individualmente. Per un contesto più approfondito, la scheda Segnali fornisce una cronologia dei segnali, come osservato da GuardDuty.

Ogni segnale, che è un GuardDuty risultato, ha il proprio livello di gravità e il proprio valore assegnati. Nella GuardDuty console, è possibile selezionare ogni segnale per visualizzare i dettagli associati.

Attori

Fornisce dettagli sugli attori della minaccia in una sequenza di attacco. Per ulteriori informazioni, consulta [Actor](#) in Amazon GuardDuty API Reference.

Endpoints

Fornisce dettagli sugli endpoint di rete utilizzati in questa sequenza di attacco. Per ulteriori informazioni, [NetworkEndpoint](#) consulta Amazon GuardDuty API Reference. Per informazioni su come GuardDuty determina la posizione, consulta [Dettagli sulla geolocalizzazione](#).

Indicatori

Include i dati osservati che corrispondono allo schema di un problema di sicurezza. Questi dati specificano il motivo per cui GuardDuty esiste un'indicazione di un'attività potenzialmente sospetta. Ad esempio, se il nome dell'indicatore è `HIGH_RISK_API`, indica un'azione comunemente utilizzata dagli autori delle minacce o un'azione sensibile che può avere un impatto potenziale su di esse Account AWS, come l'accesso alle credenziali o la modifica di una risorsa.

La tabella seguente include un elenco di potenziali indicatori e le relative descrizioni:

Nome dell'indicatore	Description
ATTACK_TACTIC	Le tattiche MITRE utilizzate dall'autore della minaccia in una sequenza di attacco. Gli esempi includono Discovery e Impact.
ATTACK_TECHNIQUE	La tecnica MITRE utilizzata dall'autore della minaccia in una sequenza di attacco. Gli esempi includono l'accesso alle risorse e il loro utilizzo involontario e lo sfruttamento delle vulnerabilità.
CRYPTOMINING_DOMAIN	Indica un nome di dominio associato a pool o infrastrutture per il mining di criptovalute. Ad esempio, le query o le connessioni DNS a questi domini da ambienti container o Kubernetes possono indicare attività di cryptomining non autorizzate.
CRYPTOMINING_IP	Indica un indirizzo IP associato a pool o infrastrutture per il mining di criptovalute. Ad esempio, le connessioni a questi indirizzi da ambienti container o Kubernetes possono indicare attività di cryptomining non autorizzate.
CRYPTOMINING_PROCESS	Indica un processo identificato come software di mining di criptovalute in esecuzione all'interno di container o ambienti Kubernetes. Ad esempio, questi processi possono consumare risorse di CPU eccessive.
HIGH_RISK_API	L' AWS API che include il Servizio AWS nome e eventName indica un'azione comunemente utilizzata dagli autori delle minacce o un'azione sensibile che può causare un potenziale impatto Account AWS, ad esempio l'accesso alle credenziali o la modifica delle risorse.
MALICIOUS_DOMAIN	Indica un nome di dominio con sospette informazioni sulle minacce che indicano intenzioni dannose. Ad esempio, ciò include server di comando e controllo (C&C), siti di distribuzione di malware o domini di phishing contattati da container o ambienti Kubernetes.
MALICIOUS_FILE	Indica un file sospettato di essere dannoso in base all'intelligence sulle minacce o all'analisi comportamentale. Ad esempio, ciò include file binari di malware noti, script dannosi o eseguibili non autorizzati.

Nome dell'indicatore	Description
MALICIOUS_IP	L'indirizzo IP ha confermato l'intelligence sulle minacce, indicando intenzioni dannose.
MALICIOUS_PROCESS	Indica un processo sospettato di essere dannoso in base all'intelligence sulle minacce o all'analisi comportamentale. Ad esempio, ciò include malware noti, backdoor o strumenti non autorizzati eseguiti all'interno di un'istanza o di un ambiente container.
SUSPICIOUS_NETWORK	La rete è associata a punteggi di reputazione noti bassi, come provider di reti private virtuali (VPN) e servizi proxy a rischio.
SUSPICIOUS_PROCESS	Indica un processo sospetto identificato come anomalo in base all'intelligence sulle minacce o all'analisi comportamentale. Ad esempio, ciò include modelli di esecuzione dei processi insoliti, relazioni padre-figlio impreviste o processi con caratteristiche sospette all'interno di un'istanza o di un ambiente contenitore.
SUSPICIOUS_USER_AGENT	Lo user agent è associato ad applicazioni sospette o sfruttate potenzialmente note, come client Amazon S3 e strumenti di attacco.
TOR_IP	L'indirizzo IP è associato a un nodo di uscita Tor.
UNUSUAL_API_FOR_ACCOUNT	Indica che l' AWS API è stata richiamata in modo anomalo, in base alla linea di base storica dell'account. Per ulteriori informazioni, consulta Comportamento anomalo .
UNUSUAL_ASN_FOR_ACCOUNT	Indica che l'Autonomous System Number (ASN) è stato identificato come anomalo, in base alla baseline storica dell'account. Per ulteriori informazioni, consulta Comportamento anomalo .
UNUSUAL_ASN_FOR_USER	Indica che l'Autonomous System Number (ASN) è stato identificato come anomalo, in base alla baseline storica dell'utente. Per ulteriori informazioni, consulta Comportamento anomalo .

Tattiche MITRE

Questo campo specifica le tattiche MITRE ATT&CK che l'autore della minaccia tenta attraverso una sequenza di attacco. GuardDuty utilizza il framework [MITRE ATT&ACK](#) che aggiunge contesto all'intera sequenza di attacco. I colori utilizzati dalla GuardDuty console per specificare gli scopi della minaccia utilizzati dall'autore della minaccia sono allineati ai colori che indicano il livello critico, alto, medio e basso. [Livelli di gravità dei risultati](#)

Indicatori di rete

Gli indicatori includono una combinazione di valori degli indicatori di rete che spiegano perché una rete è indicativa di un comportamento sospetto. Questa sezione è applicabile solo quando l'Indicatore include SUSPICIOUS_NETWORK o. MALICIOUS_IP L'esempio seguente mostra come gli indicatori di rete potrebbero essere associati a un indicatore, dove:

- *AnyCompany* è un sistema autonomo (AS).
- TUNNEL_VPNIS_ANONYMOUS, e ALLOWS_FREE_ACCESS sono gli indicatori di rete.

```
...{
  "key": "SUSPICIOUS_NETWORK",
  "values": [{
    "AnyCompany": [
      "TUNNEL_VPN",
      "IS_ANONYMOUS",
      "ALLOWS_FREE_ACCESS"
    ]
  }]
}
```

La tabella seguente include i valori degli indicatori di rete e la loro descrizione. Questi tag vengono aggiunti in base alle informazioni sulle minacce GuardDuty raccolte da fonti come Spur

Valore dell'indicatore di rete	Description
TUNNEL_VPN	L'indirizzo di rete o IP è associato a un tipo di tunnel VPN. Si riferisce a un protocollo specifico che consente di stabilire una connessione sicura e crittografata tra due punti su una rete pubblica.

Valore dell'indicatore di rete	Description
TUNNEL_PROXY	L'indirizzo di rete o IP è associato a un tipo di tunnel Proxy. Si riferisce a un protocollo specifico che consente di stabilire una connessione tramite un server proxy.
TUNNEL_RDP	L'indirizzo di rete o IP è associato all'utilizzo di un metodo di incapsulamento del traffico RDP (Remote Desktop) all'interno di un altro protocollo per migliorare la sicurezza, aggirare le restrizioni di rete o abilitare l'accesso remoto tramite firewall.
IS_ANONYMOUS	L'indirizzo di rete o IP è associato a un servizio anonimo o proxy noto. Ciò può indicare potenziali attività sospette nascoste dietro reti anonime.
KNOWN_THREAT_OPERATOR	La rete o l'indirizzo IP è associato a un provider di tunnel noto e rischioso. Ciò indica che è stata rilevata un'attività sospetta da un indirizzo IP collegato a una VPN, a un proxy o ad altri servizi di tunneling utilizzati frequentemente per scopi dannosi.
ALLOWS_FREE_ACCESS	L'indirizzo di rete o IP è associato a un operatore di tunnel che consente l'accesso al suo servizio senza richiedere l'autenticazione o il pagamento. Potrebbe includere anche account di prova o esperienze di utilizzo limitate offerte da vari servizi online.
ALLOWS_CRYPTOCURRENCY	La rete o l'indirizzo IP è associato a un provider di tunnel (come VPN o servizio proxy) che accetta esclusivamente criptovalute o altre valute digitali come metodo di pagamento.
ALLOWS_TORRENTS	L'indirizzo di rete o IP è associato a servizi o piattaforme che consentono il traffico torrent. Tali servizi sono spesso associati al supporto e all'utilizzo di torrent e ad attività di elusione del copyright.

Valore dell'indicatore di rete	Description
RISK_CALL BACK_PROXY	L'indirizzo di rete o IP è associato a dispositivi noti per indirizzare il traffico verso proxy residenziali, proxy di malware o altre reti di tipo proxy di callback. Ciò non significa che tutte le attività sulla rete siano correlate ai proxy, ma piuttosto che la rete abbia la capacità di instradare il traffico per conto di queste reti proxy.
RISK_GEO_ MISMATCH	Questo indicatore suggerisce che il centro dati o la posizione di hosting di una rete sono diversi dalla posizione prevista degli utenti e dei dispositivi che la gestiscono. Se questo valore dell'indicatore non è presente, ciò non significa che non vi sia alcuna discrepanza. Potrebbe significare che i dati non sono sufficienti per confermare la discrepanza.
IS_SCANNER	La rete o l'indirizzo IP sono associati all'esecuzione di tentativi di accesso persistenti ai moduli Web.
RISK_WEB_ SCRAPING	La rete di indirizzi IP è associata a client Web automatizzati e ad altre attività web programmatiche.
CLIENT_BE HAVIOR_FI LE_SHARING	La rete o l'indirizzo IP sono associati al comportamento del client, indicativo delle attività di condivisione di file, come reti peer-to-peer (P2P) o protocolli di condivisione di file.
CATEGORY_ COMMERCIA L_VPN	L'indirizzo di rete o IP è associato a un operatore di tunnel classificato come un tradizionale servizio VPN (Commercial Virtual Private Network) che opera all'interno dello spazio del datacenter.
CATEGORY_ FREE_VPN	L'indirizzo di rete o IP è associato a un operatore di tunnel classificato come servizio VPN completamente gratuito.
CATEGORY_ RESIDENTI AL_PROXY	L'indirizzo di rete o IP è associato a un operatore di tunnel classificato come SDK, malware o servizio proxy fornito da get-paid-to fonti.
OPERATOR_XXX	Il nome del fornitore di servizi che gestisce questo tunnel.

Dettagli utente del database (DB) RDS

Note

Questa sezione è applicabile ai risultati quando si abilita la funzionalità di protezione RDS in GuardDuty. Per ulteriori informazioni, consulta [GuardDuty Protezione RDS](#).

La GuardDuty scoperta fornisce i seguenti dettagli relativi all'utente e all'autenticazione del database potenzialmente compromesso:

- Utente: il nome utente utilizzato per effettuare il tentativo di accesso anomalo.
- Applicazione: il nome dell'applicazione utilizzata per effettuare il tentativo di accesso anomalo.
- Database: il nome dell'istanza di database coinvolta nel tentativo di accesso anomalo.
- SSL: la versione del Secure Socket Layer (SSL) utilizzata per la rete.
- Metodo di autenticazione: il metodo di autenticazione utilizzato dall'utente coinvolto nell'esito.

Per informazioni sulla risorsa potenzialmente compromessa, vedere. [Risorsa](#)

Dettagli sugli esiti del monitoraggio del runtime

Note

Questi dettagli possono essere disponibili solo se GuardDuty genera uno dei [GuardDuty Tipi di risultati del monitoraggio del runtime](#).

Questa sezione contiene i dettagli del runtime, inclusi i dettagli del processo e qualsiasi contesto richiesto. I dettagli del processo descrivono le informazioni sul processo osservato e il contesto di runtime descrive qualsiasi informazione aggiuntiva sull'attività potenzialmente sospetta.

Dettagli del processo

- Nome: il nome del processo.
- Percorso eseguibile: il percorso assoluto del file eseguibile del processo.
- SHA-256 eseguibile: l'hash SHA256 dell'eseguibile del processo.

- PID dello spazio dei nomi: l'ID processo in un PID dello spazio dei nomi secondario diverso dal PID dello spazio dei nomi a livello di host. Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
- Directory di lavoro presente: la directory di lavoro presente del processo.
- ID processo: l'ID che il sistema operativo assegna al processo.
- startTime: l'ora in cui è iniziato il processo. Si presenta nel formato della stringa di data UTC (2023-03-22T19:37:20.168Z).
- UUID: l'ID univoco assegnato al processo da GuardDuty
- UUID padre: l'ID univoco del processo padre. Questo ID viene assegnato al processo principale da GuardDuty
- Utente: l'utente che ha eseguito il processo.
- ID utente: l'ID dell'utente che ha eseguito il processo.
- ID utente effettivo: l'ID utente effettivo del processo al momento dell'evento.
- Eredità: informazioni sugli antenati del processo.
 - ID processo: l'ID che il sistema operativo assegna al processo.
 - UUID: l'ID univoco assegnato al processo da GuardDuty
 - Percorso eseguibile: il percorso assoluto del file eseguibile del processo.
 - ID utente effettivo: l'ID utente effettivo del processo al momento dell'evento.
 - UUID padre: l'ID univoco del processo padre. Questo ID viene assegnato al processo principale da GuardDuty
 - Ora di inizio: l'ora in cui è iniziato il processo.
 - PID dello spazio dei nomi: l'ID processo in un PID dello spazio dei nomi secondario diverso dal PID dello spazio dei nomi a livello di host. Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
 - ID utente: l'ID utente dell'utente che ha eseguito il processo.
 - Nome: il nome del processo.

Contesto di runtime

Un esito generato può includere, tra i campi seguenti, solo quelli pertinenti al tipo di esito.

- Origine di montaggio: il percorso sull'host montato dal container.
- Destinazione di montaggio: il percorso nel container mappato alla directory host.

- Tipo di file system: rappresenta il tipo di file system montato.
- Flag: rappresenta le opzioni che controllano il comportamento dell'evento coinvolto in questo esito.
- Processo di modifica: informazioni sul processo che in fase di runtime ha creato o modificato un file binario, uno script o una libreria all'interno di un container.
- Ora della modifica: il timestamp in cui il processo ha creato o modificato un file binario, uno script o una libreria all'interno di un container in fase di runtime. Questo campo è nel formato della stringa di data UTC (2023-03-22T19:37:20.168Z).
- Percorso libreria: il percorso della nuova libreria che è stata caricata.
- Valore LD Preload: il valore della variabile di ambiente LD_PRELOAD.
- Percorso socket: il percorso del socket Docker a cui è stato effettuato l'accesso.
- Percorso binario runc: il percorso del file binario runc.
- Percorso agente di rilascio: il percorso del file dell'agente di rilascio cgroup.
- Esempio di riga di comando: l'esempio della riga di comando coinvolta nell'attività potenzialmente sospetta.
- Categoria utensile: categoria a cui appartiene lo strumento. Alcuni esempi sono Backdoor Tool, Pentest Tool, Network Scanner e Network Sniffer.
- Nome dello strumento: il nome dello strumento potenzialmente sospetto.
- Percorso dello script: il percorso dello script eseguito che ha generato il risultato.
- Threat File Path: il percorso sospetto per il quale sono stati trovati i dettagli di intelligence sulle minacce.
- Nome del servizio: il nome del servizio di sicurezza che è stato disabilitato.
- Nome del modulo: il nome del modulo che viene caricato nel kernel.
- Modulo SHA256: l' SHA256 hash del modulo.
- Percorso del file del modulo: il percorso del modulo caricato nel kernel.

Dettagli della scansione dei volumi EBS

Note

Questa sezione è applicabile ai risultati ottenuti quando si attiva la scansione anti-malware GuardDuty avviata dall'utente. [Protezione da malware per EC2](#)

La scansione dei volumi EBS fornisce dettagli sul volume EBS collegato all'istanza EC2 o al carico di lavoro di un container potenzialmente compromessi.

- ID scansione: l'identificatore della scansione malware.
- Ora inizio scansione: la data e l'ora di inizio della scansione malware.
- Ora completamento scansione: la data e l'ora di completamento della scansione malware.
- Trigger Finding ID: l'ID di ricerca del GuardDuty risultato che ha avviato questa scansione antimalware.
- Fonti: i valori potenziali sono Bitdefender e Amazon.

Per ulteriori informazioni sul motore di scansione utilizzato per rilevare il malware, vedere [GuardDuty motore di scansione per il rilevamento di malware](#).

- Rilevamenti scansione: la visualizzazione completa dei dettagli e degli esiti di ogni scansione malware.
 - Numero elementi scansionati: il numero totale di file scansionati. Fornisce dettagli come `totalGb`, `files` e `volumes`.
 - Numero elementi rilevati come minacce: il numero totale di `files` dannosi rilevati durante la scansione.
 - Dettagli sulla minaccia con gravità più alta: i dettagli sulla minaccia di gravità più alta rilevata durante la scansione e sul numero di file dannosi. Fornisce dettagli come `severity`, `threatName` e `count`.
 - Minacce rilevate per nome: l'elemento container che raggruppa le minacce di tutti i livelli di gravità. Fornisce dettagli come `itemCount`, `uniqueThreatNameCount`, `shortened` e `threatNames`.

Dettagli sulla ricerca di Malware Protection for EC2

Note

Questa sezione è applicabile alle rilevazioni effettuate quando si attiva la scansione GuardDuty antimalware avviata. [Protezione da malware per EC2](#)

Quando la scansione Malware Protection for EC2 rileva un malware, puoi visualizzare i dettagli della scansione selezionando il risultato corrispondente nella pagina Findings della console. <https://>

console.aws.amazon.com/guardduty/ La gravità del rilevamento di Malware Protection for EC2 dipende dalla gravità del rilevamento. GuardDuty

Le seguenti informazioni sono disponibili nella sezione Minacce rilevate nel pannello dei dettagli.

- Nome: il nome della minaccia, ottenuto raggruppando i file in base al rilevamento.
- Gravità: la gravità della minaccia rilevata.
- Hash: l'hash SHA-256 del file.
- Percorso file: la posizione del file dannoso nel volume EBS.
- Nome file: il nome del file in cui è stata rilevata la minaccia.
- ARN del volume: l'ARN dei volumi EBS scansionati.

Le seguenti informazioni sono disponibili nella sezione Dettagli della scansione malware nel pannello dei dettagli.

- ID scansione: l'ID di scansione della scansione malware.
- Ora inizio scansione: la data e l'ora di inizio della scansione.
- Ora completamento scansione: la data e l'ora di completamento della scansione.
- File scansionati: il numero totale di file e directory scansionati.
- GB totali scansionati: la quantità di spazio di archiviazione scansionato durante il processo.
- Trigger Finding ID: l'ID identificativo del GuardDuty risultato che ha avviato questa scansione antimalware.
- Le seguenti informazioni sono disponibili nella sezione Dettagli del volume nel pannello dei dettagli.
 - ARN del volume: il nome della risorsa Amazon (ARN) del volume.
 - SnapshotARN: l'ARN dello snapshot del volume EBS.
 - Stato: lo stato della scansione del volume, ad esempio, Running, Skipped e Completed.
 - Tipo di crittografia: il tipo di crittografia utilizzato per crittografare il volume. Ad esempio, CMCMK.
 - Nome dispositivo: il nome del dispositivo. Ad esempio, /dev/xvda.

Dettagli sugli esiti di Malware Protection per S3

I seguenti dettagli della scansione antimalware sono disponibili quando attivi GuardDuty sia Malware Protection for S3 che su: Account AWS

- Minacce: un elenco di minacce rilevate durante la scansione del malware.

 Molteplici minacce potenziali nei file di archivio

Se hai un file di archivio contenente potenzialmente più minacce, Malware Protection for S3 segnala solo la prima minaccia rilevata. Dopodiché, lo stato della scansione viene contrassegnato come completo. GuardDuty genera il tipo di ricerca associato e invia anche EventBridge gli eventi che genera. Per ulteriori informazioni sul monitoraggio delle scansioni di oggetti Amazon S3 utilizzando gli EventBridge eventi, consulta lo schema di notifica di esempio per THREATS_FOUND in: [Risultato della scansione degli oggetti S3](#)

- Percorso dell'elemento: un elenco del percorso dell'elemento annidato e dei dettagli hash dell'oggetto S3 scansionato.
- Percorso dell'elemento annidato: percorso dell'elemento dell'oggetto S3 scansionato in cui è stata rilevata la minaccia.

Il valore di questo campo è disponibile solo se l'oggetto di primo livello è un archivio e se la minaccia viene rilevata all'interno di un archivio.

- Hash: hash della minaccia rilevata in questo risultato.
- Fonti: i valori potenziali sono Bitdefender e Amazon

Per ulteriori informazioni sul motore di scansione utilizzato per rilevare il malware, vedere [GuardDuty motore di scansione per il rilevamento di malware](#).

Azione

L'Operazione di un esito fornisce dettagli sul tipo di attività che l'ha attivato. Le informazioni disponibili variano in base al tipo di operazione.

Tipo di operazione: il tipo di attività dell'esito. Questo valore può essere NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST, _CALL o RDS_LOGIN_ATTEMPT. AWS_API Le informazioni disponibili variano in base al tipo di operazione:

- NETWORK_CONNECTION: indica che il traffico di rete è stato scambiato tra l'istanza EC2 identificata e l'host remoto. Questo tipo di operazione include le seguenti informazioni aggiuntive:
 - Direzione della connessione: la direzione della connessione di rete osservata nell'attività che ha richiesto la generazione del risultato. GuardDuty Può essere uno dei seguenti valori:

- **INBOUND:** indica che un host remoto ha avviato una connessione a una porta locale sull'istanza EC2 identificata nel tuo account.
- **OUTBOUND:** indica che l'istanza EC2 identificata ha avviato una connessione a un host remoto.
- **SCONOSCIUTA:** indica che non è GuardDuty stato possibile determinare la direzione della connessione.
- **Protocollo:** il protocollo di connessione di rete osservato nell'attività che ha richiesto GuardDuty la generazione del risultato.
- **IP locale:** il primo indirizzo IP di origine del traffico che ha attivato l'esito. Queste informazioni possono essere utilizzate per distinguere tra indirizzo IP di un livello intermedio su cui fluisce il traffico e il primo indirizzo IP di origine del traffico. Ad esempio, l'indirizzo IP di un pod EKS anziché l'indirizzo IP dell'istanza in cui è in esecuzione il pod EKS.
- **Bloccata:** indica se la porta di destinazione è bloccata.
- **PORT_PROBE:** indica che l'istanza EC2 identificata è stata sottoposta a probing da un host remoto su più porte aperte. Questo tipo di operazione include le seguenti informazioni aggiuntive:
 - **IP locale:** il primo indirizzo IP di origine del traffico che ha attivato l'esito. Queste informazioni possono essere utilizzate per distinguere tra indirizzo IP di un livello intermedio su cui fluisce il traffico e il primo indirizzo IP di origine del traffico. Ad esempio, l'indirizzo IP di un pod EKS anziché l'indirizzo IP dell'istanza in cui è in esecuzione il pod EKS.
 - **Bloccata:** indica se la porta di destinazione è bloccata.
- **DNS_REQUEST:** indica che l'istanza EC2 identificata ha eseguito query in un nome di dominio. Questo tipo di operazione include le seguenti informazioni aggiuntive:
 - **Protocollo:** il protocollo di connessione di rete osservato nell'attività che ha portato GuardDuty alla generazione del risultato.
 - **Bloccata:** indica se la porta di destinazione è bloccata.
- **AWS_API_CALL:** indica che è stata richiamata un' AWS API. Questo tipo di operazione include le seguenti informazioni aggiuntive:
 - **API:** il nome dell'operazione API che è stata richiamata e quindi ha richiesto di GuardDuty generare questo risultato.

 Note

Queste operazioni possono anche includere eventi non API acquisiti da AWS CloudTrail. Per ulteriori informazioni, consulta [Eventi non API acquisiti](#) da CloudTrail

- **Agente utente:** l'agente utente che ha effettuato la richiesta API. Questo valore indica se la chiamata è stata effettuata da Console di gestione AWS, un AWS servizio, da o da. AWS SDKs AWS CLI
- **CODICE DI ERRORE:** se l'esito è stato attivato da una chiamata API non riuscita, viene visualizzato il codice di errore per tale chiamata.
- **Nome servizio:** il nome DNS del servizio che ha tentato di effettuare la chiamata API che ha attivato l'esito.
- **RDS_LOGIN_ATTEMPT:** indica che è stato effettuato un tentativo di accesso al database potenzialmente compromesso da un indirizzo IP remoto.
- **Indirizzo IP:** l'indirizzo IP remoto utilizzato per effettuare il tentativo di accesso potenzialmente sospetto.

Attore o destinazione

Un esito ha una sezione Attore se il Ruolo risorsa era TARGET. Ciò indica che la risorsa è stata la destinazione di attività sospette e la sezione Attore contiene dettagli sull'entità che ha scelto come destinazione la risorsa.

Un esito ha una sezione Destinazione se il Ruolo risorsa era ACTOR. Ciò indica che la risorsa è stata coinvolta in attività sospette nei confronti di un host remoto e questa sezione contiene informazioni sull'IP o sul dominio di destinazione della risorsa.

Le informazioni disponibili nella sezione Attore o Destinazione possono includere quanto segue:

- **Affiliato:** indica se l' AWS account del chiamante API remoto è correlato all'ambiente in uso. GuardDuty Se questo valore è `true`, il chiamante API è affiliato in qualche modo al tuo account. Se invece il valore è `false`, il chiamante API proviene da un ambiente esterno.
- **ID account remoto:** l'ID dell'account che possiede l'indirizzo IP in uscita utilizzato per accedere alla risorsa sulla rete finale.
- **Indirizzo IP:** l'indirizzo IP coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.

- **Posizione:** informazioni sulla posizione dell'indirizzo IP coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- **Organizzazione:** informazioni sull'organizzazione dell'ISP relative all'indirizzo IP coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- **Porta:** il numero di porta coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- **Dominio:** il dominio coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- **Dominio con suffisso:** il dominio di secondo e primo livello coinvolto in un'attività che potenzialmente ha richiesto GuardDuty la generazione del risultato. [Per un elenco dei domini di primo e secondo livello, consulta l'elenco dei suffissi pubblici.](#)

Dettagli sulla geolocalizzazione

GuardDuty determina la posizione e la rete delle richieste utilizzando i database MaxMind GeoIP. MaxMind riporta un'accuratezza molto elevata dei propri dati a livello nazionale, sebbene la precisione vari in base a fattori quali il paese e il tipo di indirizzo IP.

Per ulteriori informazioni su MaxMind, consulta la sezione [Geolocalizzazione MaxMind IP](#). Se ritieni che uno qualsiasi dei dati GeoIP sia errato, invia una richiesta di [MaxMind correzione MaxMind a Correct Geo IP2](#) Data.

Informazioni aggiuntive

Tutti gli esiti hanno una sezione Informazioni aggiuntive che può includere le informazioni seguenti:

- **Nome dell'elenco delle minacce:** il nome dell'elenco delle minacce che include l'indirizzo IP o il nome di dominio coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- **Esempio:** un valore vero o falso che indica se si tratta di un esito di esempio.
- **Archiviato:** un valore vero o falso che indica se l'esito è stato archiviato.
- **Insolito:** dettagli dell'attività che non sono stati osservati in precedenza. Questi dettagli possono includere utente, posizione, bucket, comportamento di accesso od Org ASN anomali (non osservati in precedenza).
- **Protocollo insolito:** il protocollo di connessione di rete coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.

- **Dettagli dell'agente:** dettagli sull'agente di sicurezza attualmente implementato nel cluster EKS del tuo Account AWS. Questi dettagli sono applicabili solo ai tipi di esiti del monitoraggio del runtime EKS.
- **Versione dell'agente:** la versione del GuardDuty security agent.
- **ID agente:** l'identificatore univoco del GuardDuty security agent.

Evidenza

Gli esiti basati sull'intelligence sulle minacce hanno una sezione Evidenza che include le informazioni seguenti:

- **Dettagli di intelligence sulle minacce:** il nome dell'elenco delle minacce in cui Threat name compaiono le minacce riconosciute.
- **Nome della minaccia:** il nome della famiglia di malware o altro identificatore associato alla minaccia.
- **File di minaccia SHA256:** SHA256 del file che ha generato la scoperta.

Comportamento anomalo

I tipi di risultati che terminano con AnomalousBehavior indicano che il risultato è stato generato dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le richieste API al tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta.

I dettagli su quali fattori della richiesta API sono insoliti per l'identità CloudTrail dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato. Le identità sono definite dall'elemento [CloudTrail userIdentity](#) e i valori possibili sono Root::IAMUser,,, AssumedRole FederatedUser::AWSAccount, or. AWS::Service

Oltre ai dettagli disponibili per tutti i GuardDuty risultati associati all'attività dell'API, AnomalousBehavior risultati contengono dettagli aggiuntivi descritti nella sezione seguente. Questi dettagli possono essere visualizzati nella console e sono disponibili anche nel JSON dell'esito.

- **Anomalo APIs:** un elenco di richieste API richiamate dall'identità dell'utente in prossimità della richiesta API principale associata al risultato. Questo riquadro suddivide ulteriormente i dettagli dell'evento API nei modi seguenti.
 - La prima API elencata è l'API principale, ossia la richiesta API associata all'attività osservata con il rischio più elevato. Si tratta dell'API che ha attivato l'esito ed è correlata alla fase di attacco del tipo di esito. L'API in questione è descritta in dettaglio nella sezione Operazione della console e nel JSON dell'esito.
 - Tutte le altre APIs elencate sono ulteriori anomale APIs rispetto all'identità utente elencata osservata in prossimità dell'API principale. Se nell'elenco è presente una sola API, il modello di ML non ha identificato come anomala alcuna richiesta API aggiuntiva proveniente dall'identità utente.
 - L'elenco di APIs viene suddiviso in base al fatto che un'API sia stata chiamata con successo o se l'API sia stata chiamata senza successo, il che significa che è stata ricevuta una risposta di errore. Il tipo di risposta di errore ricevuta è elencato sopra ogni API chiamata senza successo. I possibili tipi di risposta di errore sono: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` e `operation not permitted`.
 - APIs sono classificati in base al servizio associato.
 - Per maggiori informazioni, scegli Cronologico APIs per visualizzare i dettagli relativi alla parte superiore APIs, fino a un massimo di 20, in genere sia per l'identità dell'utente che per tutti gli utenti all'interno dell'account. APIs Sono contrassegnati come Rari (meno di una volta al mese), Non frequenti (alcune volte al mese) o Frequenti (da giornalieri a settimanali), a seconda della frequenza con cui vengono utilizzati nell'account.
- **Comportamento insolito (account):** questa sezione fornisce ulteriori dettagli sul comportamento profilato del tuo account.

Comportamento profilato

GuardDuty impara continuamente sulle attività all'interno del tuo account in base agli eventi organizzati. Queste attività e la loro frequenza osservata sono note come comportamenti profilati.

Le informazioni registrate in questo pannello includono:

- **ASN Org:** l'organizzazione ASN (Autonomous System Number) da cui è stata effettuata la chiamata API anomala.
- **Nome utente:** il nome dell'utente che ha effettuato la chiamata API anomala.
- **Agente utente:** l'agente utente utilizzato per effettuare la chiamata API anomala. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
- **Tipo utente:** il tipo di utente che ha effettuato la chiamata API anomala. I valori possibili sono `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.
- **Bucket:** il nome del bucket S3 a cui viene effettuato l'accesso.
- **Comportamento insolito (identità utente):** questa sezione fornisce ulteriori dettagli sul comportamento profilato dell'identità utente coinvolta nell'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non aveva mai visto l'identità dell'utente effettuare questa chiamata API in questo modo durante il periodo di formazione. Sono disponibili i seguenti dettagli aggiuntivi sull'identità utente:
 - **Org ASN:** l'Org ASN da cui è stata effettuata la chiamata API anomala.
 - **Agente utente:** l'agente utente utilizzato per effettuare la chiamata API anomala. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
 - **Bucket:** il nome del bucket S3 a cui viene effettuato l'accesso.
- **Comportamento insolito (bucket):** questa sezione fornisce ulteriori dettagli sul comportamento profilato del bucket S3 associato all'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non aveva mai visto in precedenza chiamate API effettuate a questo bucket in questo modo durante il periodo di formazione. Le informazioni registrate in questa sezione includono:
 - **Org ASN:** l'Org ASN da cui è stata effettuata la chiamata API anomala.
 - **Nome utente:** il nome dell'utente che ha effettuato la chiamata API anomala.
 - **Agente utente:** l'agente utente utilizzato per effettuare la chiamata API anomala. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
 - **Tipo utente:** il tipo di utente che ha effettuato la chiamata API anomala. I valori possibili sono `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.

Note

Per maggiori informazioni sui comportamenti storici, scegli **Comportamento storico** nella sezione **Comportamento insolito (account)**, **ID utente** o **Bucket** per visualizzare i dettagli sul comportamento previsto nel tuo account per ciascuna delle seguenti categorie: **Raro (meno**

di una volta al mese), Poco frequente (alcune volte al mese) o Frequente (da giornaliero a settimanale), a seconda della frequenza con cui vengono utilizzati all'interno del tuo account.

- **Comportamento insolito (database):** questa sezione fornisce ulteriori dettagli sul comportamento profilato dell'istanza di database associata all'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non ha mai visto in precedenza un tentativo di accesso effettuato in questo modo a questa istanza di database durante il periodo di formazione. Le informazioni registrate nel pannello dell'esito per questa sezione includono:
 - **Nome utente:** il nome utente utilizzato per effettuare il tentativo di accesso anomalo.
 - **Org ASN:** l'Org ASN da cui è stato effettuato il tentativo di accesso anomalo.
 - **Nome applicazione:** il nome dell'applicazione utilizzata per effettuare il tentativo di accesso anomalo.
 - **Nome database:** il nome dell'istanza di database coinvolta nel tentativo di accesso anomalo.

La sezione **Comportamento storico** fornisce maggiori informazioni su Nomi utente, Org ASN, Nomi applicazioni e Nomi database osservati in precedenza per il database associato. A ogni valore univoco è associato un conteggio che rappresenta il numero di volte in cui questo valore è stato osservato in un evento di accesso riuscito.

- **Comportamento insolito (account cluster Kubernetes, spazio dei nomi Kubernetes e nome utente Kubernetes):** questa sezione fornisce ulteriori dettagli sul comportamento profilato per il cluster e lo spazio dei nomi Kubernetes associati all'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non ha mai osservato in precedenza questo account, cluster, namespace o nome utente in questo modo. Le informazioni registrate nel pannello dell'esito per questa sezione includono:
 - **Nome utente:** l'utente che ha chiamato l'API Kubernetes associata all'esito.
 - **Nome utente impersonato:** l'utente impersonato da `username`.
 - **Spazio dei nomi:** lo spazio dei nomi Kubernetes all'interno del cluster Amazon EKS in cui si è verificata l'operazione.
 - **Agente utente:** l'agente utente associato alla chiamata API Kubernetes. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `kubectl`.
 - **API:** l'API Kubernetes chiamata da `username` all'interno del cluster Amazon EKS.
 - **Informazioni ASN:** le informazioni ASN, come Organizzazione e ISP, associate all'indirizzo IP dell'utente che effettua questa chiamata.

- **Giorno della settimana:** il giorno della settimana in cui è stata effettuata la chiamata API Kubernetes.
- **Autorizzazione:** il verbo e la risorsa Kubernetes di cui viene verificata l'accesso per indicare se possono utilizzare o meno l'usernameAPI Kubernetes.
- **Nome dell'account di servizio:** l'account di servizio associato al carico di lavoro Kubernetes che fornisce un'identità al carico di lavoro.
- **Registro:** il registro del contenitore associato all'immagine del contenitore che viene distribuito nel carico di lavoro Kubernetes.
- **Immagine:** l'immagine del contenitore, senza i tag e il digest associati, che viene distribuita nel carico di lavoro Kubernetes.
- **Image Prefix Config:** il prefisso dell'immagine con la configurazione di sicurezza del contenitore e del carico di lavoro abilitata, ad esempio `hostNetwork privileged o`, per il contenitore che utilizza l'immagine.
- **Nome del soggetto:** i soggetti, ad esempio `usergroup`, o `serviceAccountName` che sono associati a un ruolo di riferimento in un `o. RoleBinding ClusterRoleBinding`
- **Nome del ruolo:** il nome del ruolo coinvolto nella creazione o nella modifica dei ruoli o dell'`roleBindingAPI`.

Anomalie basate sul volume S3

Questa sezione descrive in dettaglio le informazioni contestuali per le anomalie basate sul volume S3. L'esito basato sul volume ([Exfiltration:S3/AnomalousBehavior](#)) monitora il numero insolito di chiamate API S3 effettuate dagli utenti ai bucket S3, indicando una potenziale esfiltrazione di dati. Le seguenti chiamate API S3 vengono monitorate per rilevare eventuali anomalie basate sul volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Le metriche seguenti possono essere utili per creare una linea di base del comportamento abituale quando un'entità IAM accede a un bucket S3. Per identificare un'eventuale esfiltrazione di dati, l'esito del rilevamento delle anomalie basato sul volume valuta tutte le attività rispetto alla consueta linea di base comportamentale. Scegli Comportamento storico nelle sezioni Comportamento insolito

(identità utente), Volume osservato (identità utente) e Volume osservato (Bucket) per visualizzare rispettivamente le metriche seguenti.

- Numero di chiamate API `s3-api-name` richiamate dall'utente o dal ruolo IAM (in base a quello emesso) associate al bucket S3 interessato nelle ultime 24 ore.
- Numero di chiamate API `s3-api-name` richiamate dall'utente o dal ruolo IAM (in base a quello emesso) associate a tutti i bucket S3 interessati nelle ultime 24 ore.
- Numero di chiamate API `s3-api-name` su tutti gli utenti o ruoli IAM (in base a quelli emesso) associate al bucket S3 interessato nelle ultime 24 ore.

Anomalie basate sull'attività di accesso RDS

Questa sezione descrive in dettaglio il conteggio dei tentativi di accesso eseguiti dall'attore insolito ed è raggruppata in base al risultato dei tentativi di accesso. [Tipi di esiti della Protezione RDS](#) identifica comportamenti anomali monitorando gli eventi di accesso alla ricerca di schemi insoliti di `successfulLoginCount`, `failedLoginCount` e `incompleteConnectionCount`.

- `successfulLoginCount`— Questo contatore rappresenta la somma delle connessioni riuscite (combinazione corretta di attributi di accesso) effettuate all'istanza del database dall'attore insolito. Gli attributi di accesso includono nome utente, password e nome del database.
- `failedLoginCount`— Questo contatore rappresenta la somma dei tentativi di accesso falliti (non riusciti) effettuati per stabilire una connessione all'istanza del database. Ciò indica che uno o più attributi della combinazione di accesso, ad esempio nome utente, password o nome del database, erano errati.
- `incompleteConnectionCount`— Questo contatore rappresenta il numero di tentativi di connessione che non possono essere classificati come riusciti o falliti. Queste connessioni vengono chiuse prima che il database fornisca una risposta. Ad esempio, la scansione delle porte viene effettuata dove è connessa la porta del database, ma al database non viene inviata alcuna informazione oppure la connessione è stata interrotta prima del completamento di un tentativo di accesso riuscito o fallito.

GuardDuty ricerca dell'aggregazione

GuardDuty aggiorna dinamicamente i risultati generati. Se GuardDuty rileva una nuova attività correlata allo stesso problema di sicurezza, anziché creare una nuova ricerca, GuardDuty aggiornerà la scoperta originale con i dettagli più recenti. Questo comportamento consente di identificare

eventuali problemi in corso, senza la necessità di esaminare più report simili, e riduce il volume complessivo di rilevazioni relative a problemi di sicurezza noti.

Ad esempio, per quanto riguarda la UnauthorizedAccess:EC2/SSHBruteForce ricerca, più tentativi di accesso alla tua istanza verranno aggregati allo stesso ID di ricerca, aumentando il numero Count nei dettagli del risultato. Questo perché il rilevamento rappresenta un singolo problema di sicurezza con l'istanza che indica che la porta SSH sull'istanza non è adeguatamente protetta contro questo tipo di attività. Tuttavia, se GuardDuty rileva l'attività di accesso SSH che si rivolge a una nuova istanza nel proprio ambiente, verrà creato un nuovo risultato con un ID di ricerca univoco per avvisare l'utente del fatto che si è verificato un problema di sicurezza associato alla nuova risorsa.

Quando un risultato viene aggregato, viene aggiornato con le informazioni relative all'ultima occorrenza di quell'attività. Il che significa che nell'esempio precedente se la tua istanza è la destinazione di un tentativo di forza bruta da un nuovo attore, i dettagli dell'esito verranno aggiornati per riflettere l'IP remoto dell'origine più recente e le precedenti informazioni saranno sostituite. Le informazioni complete sui singoli tentativi di attività saranno ancora disponibili nei tuoi CloudTrail log o nei log di flusso VPC.

I criteri che avvisano GuardDuty di generare un nuovo risultato invece di aggregarne uno esistente dipendono dal tipo di risultato. I criteri di aggregazione per ogni tipo di risultato sono determinati dai nostri tecnici della sicurezza per fornire una panoramica dei diversi problemi di sicurezza all'interno del tuo account.

Quando viene GuardDuty generato un tipo di ricerca della sequenza di attacco nel tuo account, il risultato viene aggregato solo quando GuardDuty identifichi segnali simili nella stessa sequenza nel tuo account. Altrimenti, GuardDuty genererà un'altra sequenza di attacco.

Gestione dei GuardDuty risultati di Amazon

GuardDuty offre diverse funzioni importanti per aiutarti a ordinare, archiviare e gestire i risultati. Queste funzionalità vi aiuteranno ad adattare i risultati al vostro ambiente specifico, a ridurre il rumore derivante da risultati di scarso valore e a concentrarvi sulle minacce al vostro AWS ambiente specifico. Consulta gli argomenti di questa pagina per capire come utilizzare queste funzionalità per aumentare il valore dei risultati di sicurezza nel tuo ambiente.

Argomenti:

[Dashboard di riepilogo in Amazon GuardDuty](#)

Scopri i componenti della dashboard di riepilogo disponibile nella GuardDuty console.

[Filtrare i risultati in GuardDuty](#)

Scopri come filtrare GuardDuty i risultati in base ai criteri specificati.

[Regole di soppressione in GuardDuty](#)

Scopri come filtrare automaticamente GuardDuty gli avvisi sui risultati tramite regole di soppressione. Le regole di eliminazione archiviano automaticamente gli esiti a seconda dei filtri impostati.

[Personalizzazione del rilevamento delle minacce con elenchi di entità e elenchi di indirizzi IP](#)

Personalizza l'ambito del GuardDuty monitoraggio utilizzando elenchi di IP ed elenchi di minacce basati su indirizzi IP instradabili pubblicamente. Gli elenchi di IP affidabili impediscono la generazione di risultati non DNS a partire da IP che consideri affidabili, mentre Threat Intel Lists ti avviserà delle attività GuardDuty definite dall'utente. IPs

[Esportazione dei risultati generati su Amazon S3](#)

Esporta i risultati generati in un bucket Amazon S3 in modo da poter conservare i record oltre il periodo di conservazione dei risultati di 90 giorni. GuardDuty Utilizza questi dati storici per tenere traccia delle potenziali attività sospette nel tuo account e valutare se le misure correttive consigliate hanno avuto successo.

[Elaborazione dei GuardDuty risultati con Amazon EventBridge](#)

Imposta notifiche automatiche per GuardDuty i risultati tramite Amazon EventBridge Events. Puoi anche automatizzare altre attività EventBridge per aiutarti a rispondere ai risultati.

[Comprensione CloudWatch dei log e dei motivi per cui le risorse vengono ignorate durante la scansione Malware Protection for EC2](#)

Scopri come puoi controllare CloudWatch Logs for GuardDuty Malware Protection for EC2 e quali sono i motivi per cui l'istanza Amazon EC2 o i volumi Amazon EBS interessati potrebbero essere stati ignorati durante il processo di scansione.

[Segnalazione di falsi positivi in Malware Protection for EC2](#)

Scopri come segnalare potenziali rilevamenti di minacce false positive in Malware Protection for EC2.

[Segnalazione del risultato della scansione degli oggetti S3 come falso positivo in Malware Protection for S3](#)

Scopri come segnalare potenziali rilevamenti di minacce false positive in Malware Protection for S3.

[Segnalazione di falsi positivi in Malware Protection for Backup](#)

Scopri come segnalare potenziali rilevamenti di minacce false positive in Malware Protection for Backup.

Dashboard di riepilogo in Amazon GuardDuty

La dashboard di GuardDuty riepilogo fornisce una visualizzazione aggregata dei GuardDuty risultati generati Account AWS nel tuo documento corrente Regione AWS.

Se utilizzi un account GuardDuty amministratore, la dashboard fornisce statistiche e dati aggregati per il tuo account e gli account dei membri dell'organizzazione.

Visualizzazione della dashboard di riepilogo

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.

GuardDuty visualizza la dashboard di riepilogo per impostazione predefinita all'apertura della console.

2. Nella pagina di riepilogo, scegli la regione desiderata Regione AWS dal selettore della regione nell'angolo in alto a destra della console.

3. Dal menu di selezione dell'intervallo di date, scegli l'intervallo di date per il quale desideri visualizzare il riepilogo. Per impostazione predefinita, la dashboard mostra i dati relativi al giorno attuale, Oggi.

Note

Se non sono stati generati risultati durante l'intervallo di date selezionato, la dashboard non avrà alcun dato da visualizzare. Puoi aggiornare la dashboard o modificare l'intervallo di date.

Argomenti

- [Panoramica di](#)
- [Esiti](#)
- [Tipi di esiti più comuni](#)
- [Esiti per gravità](#)
- [Account con il maggior numero di esiti](#)
- [Risorse con esiti](#)
- [Esiti meno ricorrenti](#)
- [Copertura dei piani di protezione](#)

Panoramica di

Questa sezione fornisce i dati seguenti:

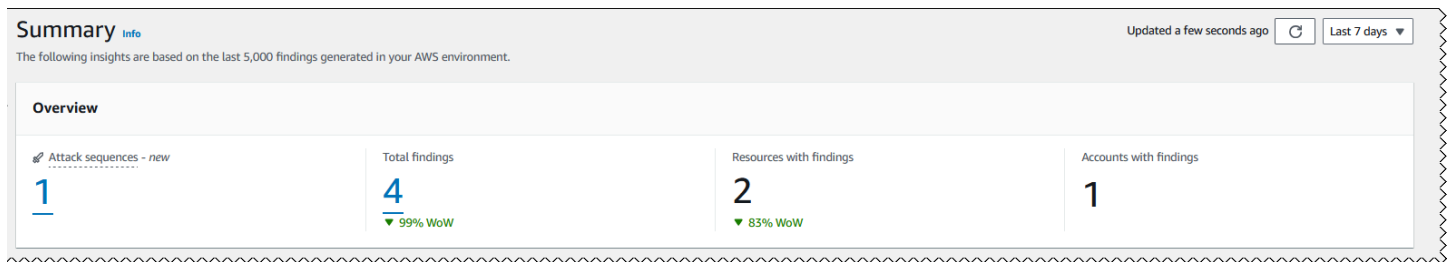
- Sequenze di attacco: indica il numero di risultati delle sequenze di attacco GuardDuty generati nel tuo account nella regione corrente.

GuardDuty rileva potenziali attacchi in più fasi nel tuo account. Puoi selezionare il numero in Sequenze di attacco per visualizzarne i dettagli nella pagina Risultati.

- Esiti totali: indica il numero totale di esiti generati nel tuo account nella regione attuale. Ciò include sia i risultati individuali che i risultati delle sequenze di attacco.
- Risorse con risultati: indica il numero di risorse associate a un risultato e che sono state potenzialmente compromesse.

- **Account con esiti:** indica il numero di account in cui è stato generato almeno un esito. Se sei un account indipendente, il valore di questo campo è 1.

Per gli intervalli di tempo Ultimi 7 giorni e Ultimi 30 giorni, il riquadro Panoramica può mostrare la differenza percentuale rispettivamente degli esiti generati settimanalmente (WoW) o mensilmente (MoM). Se non sono stati generati esiti nella settimana o nel mese precedente, in assenza quindi di dati da confrontare, la differenza percentuale potrebbe non essere disponibile.



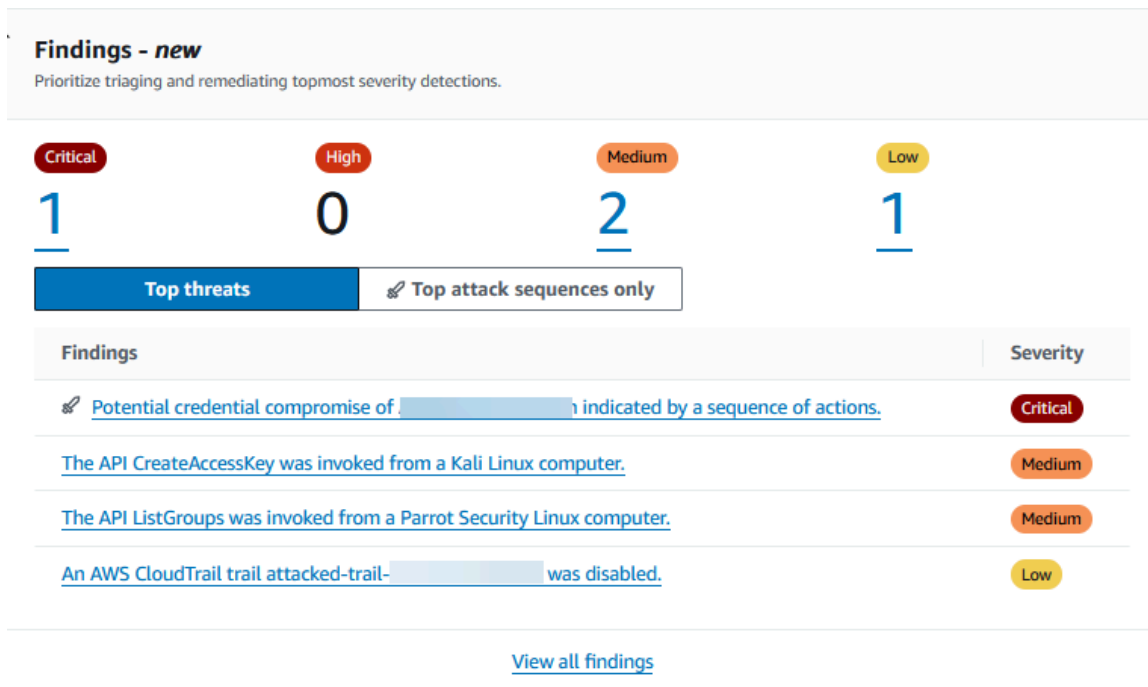
Se sei un account GuardDuty amministratore, tutti questi campi forniscono i dati riepilogati di tutti gli account membro della tua organizzazione.

Esiti

Il widget Findings mostra fino a otto risultati principali. Questi risultati sono elencati in base al loro livello di gravità, con i risultati critici visualizzati per primi.

Per impostazione predefinita, puoi visualizzare tutti i risultati. Per visualizzare solo i dati relativi ai risultati delle sequenze di attacco, attiva Solo le sequenze di attacco principali.

In questo elenco, puoi selezionare qualsiasi risultato per visualizzarne i dettagli.



Tipi di esiti più comuni

Questa sezione fornisce un grafico a torta che illustra i cinque tipi di risultati più comuni generati nella regione corrente. Passando il mouse su ogni settore del grafico a torta, puoi osservare quanto segue:

- **Conteggio dei risultati:** indica il numero di volte in cui questo risultato è stato generato nell'intervallo di date scelto.
- **Severità:** indica il livello di gravità del risultato.
- **Percentuale:** indica la proporzione di questo tipo di risultato rispetto al totale.
- **Ultima generazione:** indica quanto tempo è trascorso dall'ultima volta che questo tipo di risultato è stato rilevato.

Esiti per gravità

Questa sezione mostra un grafico a barre che mostra il numero totale di risultati nell'intervallo di date selezionato. Il grafico suddivide i risultati per gravità (critica, alta, media e bassa) e consente di visualizzare il numero di risultati per date specifiche all'interno dell'intervallo.

Per visualizzare i conteggi per ogni livello di gravità in una data specifica, passa il mouse sulla barra corrispondente nel grafico.

Account con il maggior numero di esiti

Questa sezione fornisce i dati seguenti:

- **Account:** indica l' Account AWS ID in cui è stata generata la scoperta.
- **Conteggio dell'esito:** indica il numero di volte in cui è stato generato un esito per questo ID account.
- **Ultima generazione:** indica quanto tempo è trascorso dall'ultima generazione di un tipo di esito per questo ID account.
- **Filtro di severità:** per impostazione predefinita, vengono visualizzati i dati per i tipi di risultati ad alta gravità. Le opzioni possibili per questo campo sono Tutte le severità, Gravità critica, Severità elevata e Severità media.

Risorse con esiti

Questa sezione fornisce i dati seguenti:

- **Risorsa:** mostra il tipo di risorsa potenzialmente interessata e, se questa risorsa appartiene al tuo account, puoi accedere al collegamento rapido per visualizzare i dettagli della risorsa. Se sei un account GuardDuty amministratore, puoi visualizzare i dettagli della risorsa potenzialmente interessata accedendo alla GuardDuty console con le credenziali dell'account membro proprietario.
- **Account:** indica l' Account AWS ID a cui appartiene questa risorsa.
- **Conteggio dell'esito:** indica il numero di volte in cui questa risorsa è stata associata a un esito.
- **Ultima generazione:** indica quanto tempo è trascorso dall'ultima generazione di un tipo di esito associato a questa risorsa.
- **Filtro per tipo di risorsa:** per impostazione predefinita, i dati vengono visualizzati per tutti i tipi di risorse. Utilizzando questo filtro, puoi scegliere di visualizzare i dati per un tipo di risorsa specifico, come Instance AccessKey, Lambda e altri.
- **Filtro di severità:** per impostazione predefinita, i dati vengono visualizzati per Tutti i livelli di gravità. Utilizzando questo filtro, è possibile scegliere di visualizzare i dati per altri livelli di gravità. Le opzioni possibili sono Severità critica, Severità elevata, Severità media e Gravità totale.

Esiti meno ricorrenti

Questa sezione evidenzia l'individuazione di tipi che si verificano raramente nell' AWS ambiente in uso. Questo widget è progettato per aiutarti a identificare e indagare sui potenziali modelli di minaccia emergenti.

Questo widget mostra i seguenti dati:

- Tipo di ricerca: mostra il nome del tipo di ricerca.
- Conteggio dell'esito: indica il numero di volte in cui questo esito è stato generato nell'intervallo di tempo selezionato.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di questo tipo di esito.
- Filtro di gravità: per impostazione predefinita, vengono visualizzati i dati per i tipi di risultati con livello di gravità elevato. Le opzioni possibili per questo campo sono Severità critica, Severità elevata, Severità media e Gravità totale.

Copertura dei piani di protezione

Questa sezione mostra le statistiche relative agli account dei membri dell'organizzazione. Mostra il numero di account membro che sono stati abilitati GuardDuty (rilevamento delle minacce fondamentali) nella regione corrente. Solo un GuardDuty amministratore delegato può visualizzare le statistiche relative agli account dei membri all'interno della propria organizzazione. Quando si crea una nuova AWS organizzazione, potrebbero essere necessarie fino a 24 ore per generare le statistiche per l'intera organizzazione.

Come usare questo widget

- Configurazione: se non è configurato un piano di protezione, scegli Configura nella colonna Azioni.
- Visualizzazione degli account abilitati: passa il mouse sulla barra nella colonna Account abilitati per visualizzare quanti account hanno abilitato ciascun piano di protezione. Per visualizzare ulteriormente i dettagli dell'account, seleziona la barra verde e scegli Visualizza account.

Protection plans coverage Last updated: 3 hours ago

GuardDuty coverage (foundational)
[4/4 accounts](#)

Protection plan	Enabled accounts	Actions
S3 Protection		Configure
EKS Protection		Configure
Runtime monitoring		Runtime monitoring Enabled accounts 1 Not enabled accounts 3 Configure View accounts
Automated agent management for EKS		
Automated agent configuration for Fargate (ECS only)		
Automated agent management for EC2		Configure
Malware Protection for EC2		Configure
Lambda Protection		Configure
RDS Protection		Configure

Filtrare i risultati in GuardDuty

Un filtro per gli esiti ti consente di visualizzare gli esiti che corrispondono ai criteri specificati e di escludere gli esiti non corrispondenti. Puoi creare facilmente filtri di ricerca utilizzando la GuardDuty console Amazon oppure puoi crearli con l'[CreateFilter](#) API utilizzando JSON. Consulta le sezioni seguenti per capire come creare un filtro nella console. Per utilizzare questi filtri in modo da archiviare automaticamente gli esiti in arrivo, consulta [Regole di soppressione in GuardDuty](#).

Quando crei filtri, prendi in considerazione il seguente elenco:

- Puoi specificare da uno a 50 attributi come criteri per un determinato filtro.
- Quando si utilizza l'operatore Uguale o Non è uguale per filtrare in base al valore di un attributo, ad esempio Account ID, è possibile specificare un massimo di 50 valori.
- Ogni attributo dei criteri di filtro viene valutato come operatore AND. Più valori per lo stesso attributo vengono valutati come AND/OR.
- Per informazioni sul numero massimo di filtri salvati che è possibile creare in ciascuno di essi, vedere Account AWS . Regione AWS [GuardDuty quote](#)

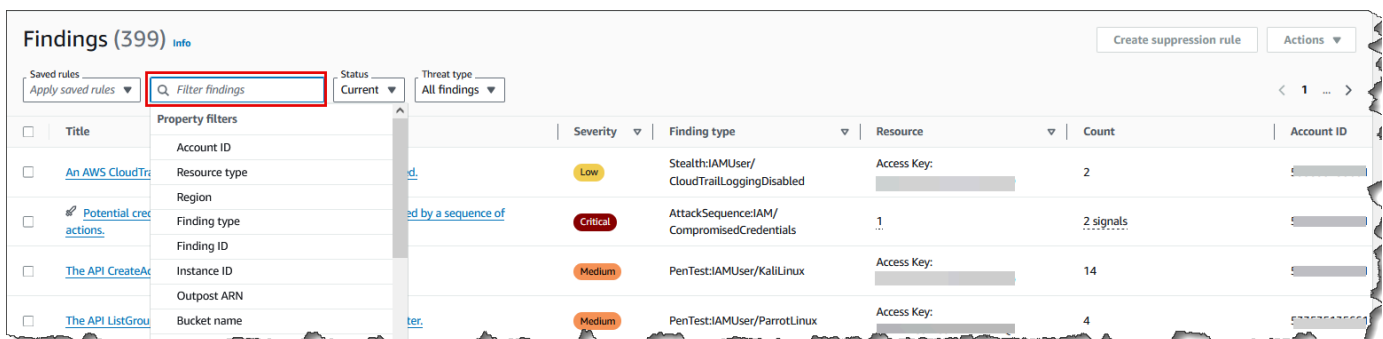
Le seguenti sezioni forniscono istruzioni su come creare e salvare filtri utilizzando la GuardDuty console e i comandi API e CLI. Scegli il metodo di accesso preferito per procedere.

Creazione e salvataggio del set di filtri nella GuardDuty console

I filtri di ricerca possono essere creati e testati tramite la GuardDuty console. Puoi salvare i filtri che hai creato tramite la console per utilizzarli nelle regole di eliminazione o nelle operazioni di filtro future. Un filtro è composto da almeno un criterio di filtro, che consiste in un attributo del filtro abbinato ad almeno un valore.

Per creare e salvare i criteri di filtro (console)

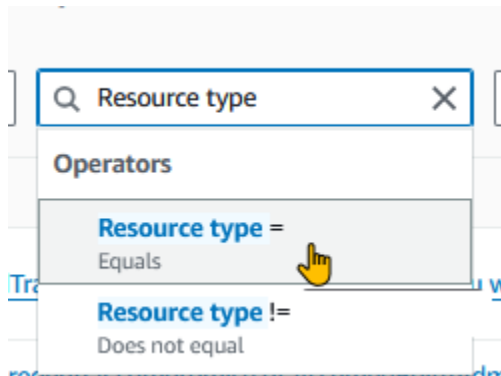
1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione a sinistra, scegli Findings.
3. Nella pagina Risultati, seleziona la barra dei risultati del filtro accanto al menu Regole salvate. Verrà visualizzato un elenco esteso di filtri di proprietà.



4. Dall'elenco esteso di filtri, selezionate un attributo in base al quale filtrare la tabella dei risultati.

Ad esempio, per visualizzare i risultati per i quali la risorsa potenzialmente interessata è un S3Bucket, scegli Tipo di risorsa.

5. Per Operatori, scegli uno che ti aiuti a filtrare i risultati per ottenere il risultato desiderato. Per continuare l'esempio del passaggio precedente, scegli Tipo di risorsa =. Verrà visualizzato un elenco di tipi di risorse in GuardDuty.



Se il tuo caso d'uso richiede l'esclusione di risultati specifici, puoi scegliere Non è uguale a o != operatore.

6. Specificate il valore per il filtro delle proprietà selezionato. Se necessario, scegliete Applica. Per continuare l'esempio del passaggio precedente, puoi scegliere S3Bucket.

Questo mostrerà i risultati che corrispondono ai filtri applicati.

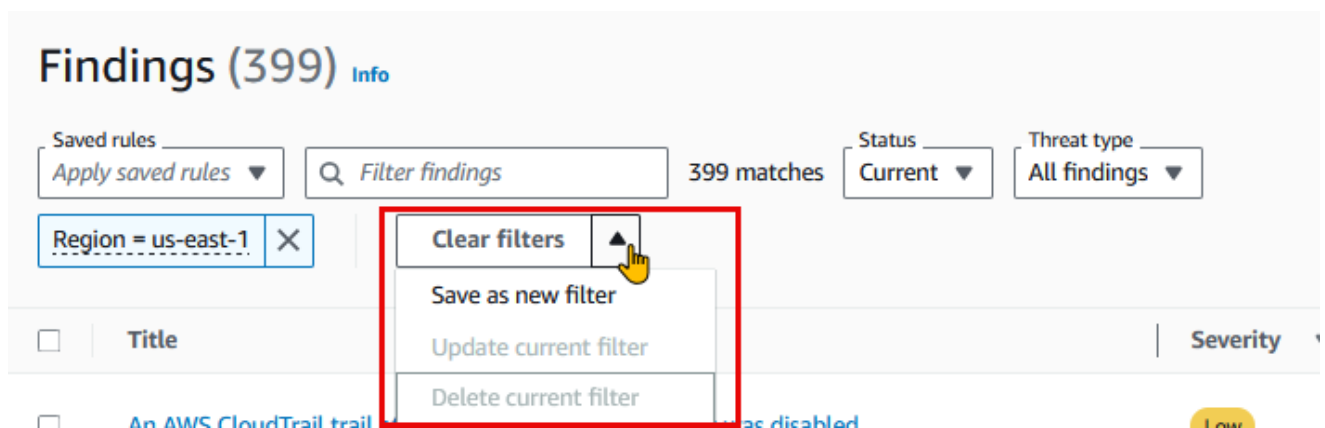
7. Per aggiungere più di un criterio di filtro, ripeti i passaggi 3-6.

Per un elenco completo degli attributi, vedere [Filtri di proprietà in GuardDuty](#).

8. (Facoltativo) salva gli attributi e i valori specificati come filtri

Per applicare nuovamente questa combinazione di filtri in futuro, è possibile salvare gli attributi specificati e i relativi valori come set di filtri.

- a. Dopo aver creato un criterio di filtro con uno o più filtri di proprietà, selezionate la freccia nel menu Cancella filtri.



- b. Inserisci il nome del set di filtri. Il nome deve contenere da 3 a 64 caratteri. I caratteri validi sono A-Z, a-z, 0-9, trattino (-), trattino basso (_) e punto (.).

- c. La descrizione è facoltativa. Se inserisci una descrizione, questa può contenere fino a 512 caratteri.
- d. Scegli Create (Crea).

Creazione e salvataggio di set di filtri utilizzando GuardDuty API e CLI

Puoi creare e testare i filtri di ricerca utilizzando i comandi API o CLI. Un filtro è composto da almeno un criterio di filtro, che consiste in un attributo del filtro abbinato ad almeno un valore. È possibile salvare i filtri per creare [Regole di eliminazione](#) o eseguire altre operazioni di filtro in un secondo momento.

Per creare filtri di ricerca utilizzando API/CLI

- Esegui l'[CreateFilter](#) API utilizzando l'ID del rilevatore regionale del Account AWS punto in cui desideri creare un filtro.

Per trovare il codice detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

- In alternativa, puoi utilizzare la [CLI create-filter](#) per creare e salvare il filtro. È possibile utilizzare uno o più criteri di filtro da. [Filtri di proprietà in GuardDuty](#)

Utilizza i seguenti esempi sostituendo i valori segnaposto mostrati in rosso.

Esempio 1: crea un nuovo filtro per visualizzare tutti i risultati che corrispondono a un tipo di risultato specifico

L'esempio seguente crea un filtro che corrisponde a tutti i PortScan risultati di un'istanza creata da un'immagine specifica. I valori segnaposto sono mostrati in rosso. Sostituisci questi valori con valori adatti al tuo account. Ad esempio, sostituiscilo **12abc34d567e8fa901bc2d34EXAMPLE** con il tuo ID regionale del rilevatore.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},  
"resource.instanceDetails.imageId": {"Equals":["ami-0a7a207083example"]}} }'
```

Esempio 2: crea un nuovo filtro per visualizzare tutti i risultati che corrispondono ai livelli di gravità

L'esempio seguente crea un filtro che corrisponde a tutti i risultati associati ai livelli di HIGH gravità. I valori segnaposto sono mostrati in rosso. Sostituisci questi valori con valori adatti al tuo account. Ad esempio, sostituiscilo `12abc34d567e8fa901bc2d34EXAMPLE` con il tuo ID regionale del rilevatore.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Per API/CLI, [Livelli di gravità dei risultati](#) sono rappresentati come numeri. Per filtrare i risultati in base ai livelli di gravità, utilizza i seguenti valori:
 - Per i livelli di LOW gravità, usa { "severity": { "Equals": ["1", "2", "3"] } }
 - Per i livelli di MEDIUM gravità, utilizzare { "severity": { "Equals": ["4", "5", "6"] } }
 - Per i livelli di HIGH gravità, utilizzare { "severity": { "Equals": ["7", "8"] } }
 - Per i livelli di CRITICAL gravità, utilizzare { "severity": { "Equals": ["9", "10"] } }
 - Per i risultati con più livelli di gravità, utilizzate valori segnaposto simili all'esempio seguente: { "severity": { "Equals": ["7", "8", "9", "10"] } }

Questo esempio mostrerà i risultati con uno HIGH o più livelli di CRITICAL gravità.

Note

Se si specifica un esempio con un solo valore numerico anziché tutti i valori numerici associati a un livello di gravità, l'API e la CLI potrebbero mostrare i risultati filtrati. Quando utilizzi questo set di filtri salvato nella GuardDuty console, non funzionerà come previsto. Questo perché la GuardDuty console considera i valori del filtro come CRITICALHIGH, MEDIUM, e LOW. Ad esempio, un filtro creato con un comando CLI che include { "severity": { "Equals": ["9"] } } dovrebbe mostrare un output appropriato in API/CLI. Tuttavia, questo filtro salvato include un livello di gravità parziale se utilizzato nella GuardDuty console e non mostrerà l'output previsto. Ciò rende necessario che l'API e la CLI specifichino tutti i valori associati a ciascun livello di gravità.

Filtri di proprietà in GuardDuty

Quando crei filtri o ordini gli esiti utilizzando le operazioni API, devi specificare i criteri di filtro in JSON. Questi criteri di filtro sono correlati al JSON dei dettagli di un esito. La tabella seguente contiene un elenco dei nomi che vengono visualizzati nella console per gli attributi dei filtri e i nomi dei campi JSON equivalenti.

Nome campo console	Nome campo JSON
ID account	accountId
ID risultato	id
Region	region
Gravità	severity È possibile filtrare i tipi di risultati in base al livello di gravità dei tipi di risultati. Per ulteriori informazioni sui valori di gravità, vedere Livelli di gravità dei risultati GuardDuty . Se si utilizza severity con l'API AWS CLI, o CloudFormation, viene assegnato un valore numerico. Per ulteriori informazioni, consulta FindingCriteria nell'Amazon GuardDuty API Reference.
Tipo di risultato	tipo
Ora aggiornamento	updatedAt
ID chiave di accesso	risorsa. accessKeyDetails. accessKeyId
ID principale	risorsa. accessKeyDetails. ID principale
Username	risorsa. accessKeyDetails.Nome utente
Tipo di utente	risorsa. accessKeyDetails.tipo di utente
ID profilo dell'istanza IAM	Resource.InstanceDetails. iamInstanceProfile .id

Nome campo console	Nome campo JSON
ID istanza	resource.instanceDetails.instanceId
ID immagine istanza	resource.instanceDetails.imageId
Chiave di tag dell'istanza	resource.instanceDetails.tags.key
Valore del tag dell'istanza	resource.instanceDetails.tags.value
IPv6 indirizzo	resource.instanceDetails.networkInterfaces.ipv6Addresses
IPv4 Indirizzo privato	Resource.InstanceDetails.Interfacce di rete. privateIpAddresses. privateIpAddress
Nome DNS pubblico	Resource.InstanceDetails.Interfacce di rete. publicDnsName
IP pubblico	resource.instanceDetails.networkInterfaces.publicIp
ID gruppo di sicurezza	resource.instanceDetails.networkInterfaces.securityGroups.groupId
Nome del gruppo di sicurezza	resource.instanceDetails.networkInterfaces.securityGroups.groupName
ID sottorete	resource.instanceDetails.networkInterfaces.subnetId
ID VPC	resource.instanceDetails.networkInterfaces.vpcId
ARN dell'Outpost	resource.instanceDetails.outpostARN
Tipo di risorsa	resource.resourceType
Autorizzazioni del bucket	resource.s3.publicAccess.EffectivePermission BucketDetails

Nome campo console	Nome campo JSON
Nome bucket	risorse.s3 .nome BucketDetails
Chiave tag bucket	risorse.s3 .tags.key BucketDetails
Valore tag bucket	risorse.s3 .tags.value BucketDetails
Tipo di bucket	risorse.s3 .type BucketDetails
Tipo di operazione	service.action.actionType
API chiamata	servizio.azione. awsApiCallAzione.api
Tipo intermediario API	servizio.azione. awsApiCallaction.callerType
Codice di errore API	servizio.azione. awsApiCallcodice di errore action.error
Città intermediario API	servizio.azione. awsApiCallAzione. remotelpD etails.città.Nome della città
Paese intermediario API	servizio.azione. awsApiCallAzione. remotelpD etails.Paese.CountryName
Indirizzo API del chiamante IPv4	service.action. awsApiCallAzione. remotelpD etails.Indirizzo IP v4
Indirizzo del chiamante API IPv6	service.action. awsApiCallAzione. remotelpD etails.indirizzo IP v6
ID ASN intermediario API	servizio.azione. awsApiCallAzione. remotelpD etails.organizzazione.asn
Nome ASN intermediario API	servizio.azione. awsApiCallAzione. remotelpD etails.Organizzazione.asnorg
Nome del servizio intermediario API	servizio.azione. awsApiCallaction.serviceName
Dominio richiesta DNS	servizio.azione. dnsRequestAction.dominio

Nome campo console	Nome campo JSON
Suffisso del dominio richiesta DNS	servizio.azione. dnsRequestAction. domainWithSuffix
Connessione di rete bloccata	servizio.azione. networkConnectionAction.bloccato
Direzione connessione rete	servizio.azione. networkConnectionAction. Direzione della connessione
Porta locale connessione rete	servizio.azione. networkConnectionAction. localPortDetails.porta
Protocollo connessione rete	servizio.azione. networkConnectionAction.protocollo
Città connessione di rete	servizio.azione. networkConnectionAction. remotelpDetails.città. Nome della città
Paese connessione di rete	servizio.azione. networkConnectionAction. remotelpDetails.Paese. Nome del Paese
Indirizzo remoto della connessione di rete IPv4	servizio.azione. networkConnectionAction. remotelpDetails.indirizzo IP v4
Indirizzo remoto della connessione di rete IPv6	servizio.azione. networkConnectionAction. remotelpDetails.indirizzo IP v6
ID ASN IP remoto connessione rete	servizio.azione. networkConnectionAction. remotelpDetails.organizzazione.asn
Nome ASN IP remoto connessione rete	servizio.azione. networkConnectionAction. remotelpDetails.Organizzazione.asnorg
Porta remota connessione rete	servizio.azione. networkConnectionAction. remotePortDetails.porta
Account remoto affiliato	servizio.azione. awsApiCallAzione. remoteAccountDetails.affiliato

Nome campo console	Nome campo JSON
Indirizzo del chiamante dell'API Kubernetes IPv4	servizio.azione. kubernetesApiCallAzione. remotelpDetails.Indirizzo IP v4
Indirizzo del chiamante dell'API Kubernetes IPv6	servizio.azione. kubernetesApiCallAzione. remotelpDetails.indirizzo IP v6
Spazio dei nomi Kubernetes	servizio.azione. kubernetesApiCallAction.nam espace
ID ASN chiamante API Kubernetes	servizio.azione. kubernetesApiCallAzione. remotelpDetails.organizzazione.asn
URI della richiesta di chiamata API Kubernetes	servizio.azione. kubernetesApiCallazione. RequestURI
Codice di stato API Kubernetes	servizio.azione. kubernetesApiCallcodice action.status
Indirizzo locale della connessione di rete IPv4	service.action. networkConnectionAction. localIpDetails.indirizzo IP v4
Indirizzo locale della connessione di rete IPv6	service.action. networkConnectionAction. localIpDetails.indirizzo IP v6
Protocollo	servizio.azione. networkConnectionAction.pro tocollo
Nome servizio chiamata API	servizio.azione. awsApiCallaction.serviceName
ID account chiamante API	servizio.azione. awsApiCallAzione. remoteAcc ountDetails.ID account
Nome elenco minacce	Servizio. Informazioni aggiuntive. threatLis tName
Ruolo risorsa	service.resourceRole
Nome del cluster EKS	risorsa. eksClusterDetails.nome

Nome campo console	Nome campo JSON
Nome del carico di lavoro Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.nome
Spazio dei nomi del carico di lavoro Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.namespace
Nome utente Kubernetes	Resource.KubernetesDetails. kubernete sUserDetails.nome utente
Immagine del container di Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.contenitori.immagine
Prefisso dell'immagine del container di Kubernetes	Resource.kubernetesDetails. kubernete sWorkloadDetails.Contenitori.Image Prefix
ID scansione	servizio. ebsVolumeScanDettagli.scanID
Nome della minaccia di scansione del volume EBS	servizio. ebsVolumeScanDettagli.ScanD etections. threatDetectedByNome.Threat Names.Name
Nome della minaccia di scansione degli oggetti S3	servizio. malwareScanDetails.threats.name
Gravità delle minacce	servizio. ebsVolumeScanDettagli.ScanD etections. threatDetectedByNome. Nomi delle minacce. Severità
File SHA	servizio. ebsVolumeScanDettagli.ScanD etections. threatDetectedByNome.Threat Names.FilePaths.Hash
Nome del cluster ECS	risorsa. ecsClusterDetails.nome
Immagine del container ECS	risorsa. ecsClusterDetails.taskdetails.contai ners.image

Nome campo console	Nome campo JSON
ARN di definizione del processo ECS	risorsa. ecsClusterDetails.taskdetails.definitionARN
Immagine del container autonomo	resource.containerDetails.image
ID istanza di database	risorsa. rdsDbInstanceDettagli. dbInstanceIdentifier
ID del cluster di database	risorsa. rdsDbInstanceDettagli. dbClusterIdentifier
Motore di database	risorsa. rdsDbInstanceDettagli. Motore
Utente del database	risorsa. rdsDbUserDettagli. Utente
Chiave di tag dell'istanza database	risorsa. rdsDbInstancedetails.tags.key
Valore del tag dell'istanza database	risorsa. rdsDbInstancedetails.tags.value
SHA-256 eseguibile	service.runtimeDetails.process.executableSha256
Process name (Nome del processo)	service.runtimeDetails.process.name
Percorso eseguibile	service.runtimeDetails.process.executablePath
Nome della funzione Lambda	resource.lambdaDetails.functionName
ARN della funzione Lambda	resource.lambdaDetails.functionArn
Chiave di tag con funzione Lambda	resource.lambdaDetails.tags.key
Valore del tag della funzione lambda	resource.lambdaDetails.tags.value
Dominio richiesta DNS	servizio.azione. dnsRequestAction. domainWithSuffix

Regole di soppressione in GuardDuty

Una regola di eliminazione è un insieme di criteri in cui ogni attributo di filtro è abbinato a un valore. Questi criteri vengono utilizzati per filtrare gli esiti, archiviando automaticamente i nuovi esiti che corrispondono ai criteri specificati. Le regole di soppressione possono essere utilizzate per filtrare risultati di basso valore, risultati falsi positivi o minacce su cui non si intende agire, per facilitare il riconoscimento delle minacce alla sicurezza con l'impatto maggiore sull'ambiente.

Dopo aver creato una regola di soppressione, i nuovi risultati che corrispondono ai criteri definiti nella regola vengono archiviati automaticamente finché la regola di soppressione è in vigore. Puoi utilizzare un filtro esistente per creare una regola di eliminazione oppure puoi crearne una a partire da un nuovo filtro definito. È possibile configurare le regole di eliminazione in modo da eliminare interi tipi di risultati oppure definire criteri di filtro più granulari per sopprimere solo istanze specifiche di un particolare tipo di risultato. È possibile modificare le regole di soppressione in qualsiasi momento.

I risultati soppressi non vengono inviati ad AWS Security Hub CSPM Amazon Simple Storage Service, Amazon Detective o Amazon EventBridge, riducendo il livello di rumore delle ricerche se si utilizzano GuardDuty i risultati tramite Security Hub CSPM, un SIEM di terze parti o altre applicazioni di avviso e ticketing. Se l'hai abilitato [Protezione da malware per EC2](#), i GuardDuty risultati soppressi non avvieranno una scansione antimalware.

GuardDuty continua a generare risultati anche quando corrispondono alle regole di soppressione impostate, tuttavia tali risultati vengono automaticamente contrassegnati come archiviati. I risultati archiviati vengono archiviati GuardDuty per 90 giorni e possono essere visualizzati in qualsiasi momento durante tale periodo. Puoi visualizzare i risultati soppressi nella GuardDuty console selezionando Archiviato dalla tabella dei risultati o tramite l' GuardDuty API utilizzando l'[ListFindings](#) API con un `findingCriteria` criterio uguale a `true.service.archived`

Note

In un ambiente con più account solo l' GuardDuty amministratore può creare regole di soppressione.

Utilizzo delle regole di soppressione con Extended Threat Detection

GuardDuty Extended Threat Detection rileva automaticamente gli attacchi in più fasi che riguardano fonti di dati, più tipi di AWS risorse e tempi, all'interno di un unico. Account AWS Mette in correlazione

gli eventi tra diverse fonti di dati per identificare gli scenari che si presentano come una potenziale minaccia per AWS l'ambiente e quindi genera una ricerca della sequenza di attacco. Per ulteriori informazioni, consulta [Come funziona Extended Threat Detection](#).

Quando si creano regole di soppressione che archiviano i risultati, Extended Threat Detection non può utilizzare questi risultati archiviati per correlare gli eventi per le sequenze di attacco. Le regole di soppressione generali potrebbero influire sulla capacità di rilevare comportamenti in linea con il rilevamento degli attacchi GuardDuty in più fasi. I risultati archiviati in base alle regole di soppressione non sono considerati segnali per le sequenze di attacchi. Ad esempio, se crei una regola di soppressione che archivia tutti i risultati relativi al cluster EKS invece di indirizzare attività specifiche note, non GuardDuty sarai in grado di utilizzare tali risultati per rilevare una sequenza di attacco in cui un autore della minaccia sfrutta un contenitore, ottiene token privilegiati e accede a risorse sensibili.

Prendi in considerazione i seguenti consigli di: GuardDuty

- Continuate a utilizzare le regole di soppressione per ridurre gli avvisi provenienti da attività affidabili note.
- Mantieni le regole di soppressione incentrate su comportamenti specifici per i quali non desideri GuardDuty generare risultati.

Casi d'uso comuni per le regole di eliminazione ed esempi

I seguenti tipi di risultati presentano casi d'uso comuni per l'applicazione delle regole di soppressione. Seleziona il nome del risultato per saperne di più su tale risultato. Esamina la descrizione del caso d'uso per decidere se creare una regola di soppressione per quel tipo di risultato.

Important

GuardDuty consiglia di creare regole di soppressione in modo reattivo e solo per i risultati per i quali sono stati ripetutamente identificati falsi positivi nel proprio ambiente.

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#): utilizza una regola di eliminazione per archiviare automaticamente gli esiti generati quando la rete VPC è configurata per instradare il traffico Internet in modo tale che esso esca da un gateway on-premise anziché da un gateway Internet VPC.

Questo esito viene generato quando la rete è configurata per instradare il traffico Internet in modo tale da uscire da un gateway on-premise anziché da un gateway Internet (IGW) VPC. Configurazioni comuni, come l'utilizzo di [AWS Outposts](#) o delle connessioni VPN del VPC, possono instradare il traffico in questo modo. Se questo è il comportamento previsto, si consiglia di utilizzare le regole di soppressione e di creare una regola composta da due criteri di filtro. Il primo criterio è tipo di esito, che dovrebbe essere `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'IPv4 indirizzo del chiamante API con l'indirizzo IP o l'intervallo CIDR del gateway Internet locale. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base all'indirizzo IP del chiamante API.

Finding type: `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`
API caller IPv4 address: `198.51.100.6`

 Note

Per includere più chiamanti API, IPs puoi aggiungere un nuovo filtro di indirizzo API Caller IPv4 per ciascuno.

- [Recon:EC2/Portscan](#): utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando utilizzi un'applicazione di valutazione della vulnerabilità.

La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `Recon:EC2/Portscan`. Il secondo criterio di filtro dovrebbe corrispondere all'istanza o alle istanze che ospitano questi strumenti di valutazione della vulnerabilità. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda dei criteri identificabili con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con determinate AMI.

Finding type: `Recon:EC2/Portscan` Instance image ID: `ami-999999999`

- [UnauthorizedAccess:EC2/SSHBruteForce](#): utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando è destinata a istanze di host bastione.

Se l'obiettivo del tentativo di forza bruta è un bastion host, ciò potrebbe rappresentare il comportamento previsto per l'ambiente in uso. AWS In questo caso, si consiglia di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita

da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `UnauthorizedAccess:EC2/SSHBruteForce`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da host bastione. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con un determinato valore del tag dell'istanza.

Finding type: *UnauthorizedAccess:EC2/SSHBruteForce* Instance tag value: *devops*

- [Recon:EC2/PortProbeUnprotectedPort](#): utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando è destinata a istanze esposte intenzionalmente.

Tuttavia, ci possono essere casi in cui le istanze sono intenzionalmente esposte, ad esempio se ospitano server web. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di esito con un valore di `Recon:EC2/PortProbeUnprotectedPort`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da host bastione. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con una determinata chiave di tag dell'istanza nella console.

Finding type: *Recon:EC2/PortProbeUnprotectedPort* Instance tag key: *prod*

Regole di soppressione consigliate per i risultati del Runtime Monitoring

- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#) viene generato quando un processo all'interno di un container comunica con il socket Docker. Nel tuo ambiente potrebbero esserci container che devono accedere al socket Docker per motivi legittimi. L'accesso da parte di tali container genererà esiti `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Se questo è un caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo tipo di risultati. Il primo criterio dovrebbe utilizzare il campo Tipo di risultato con valore uguale a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Il secondo criterio di filtro è il campo Percorso eseguibile con valore uguale al `executablePath` del processo nell'esito generato. In alternativa, il secondo criterio di filtro può utilizzare il campo SHA-256 eseguibile con valore uguale al `executableSha256` del processo nell'esito generato.

- I cluster Kubernetes gestiscono i propri server DNS come pod, ad esempio. coredns. Pertanto, per ogni ricerca DNS da un pod, GuardDuty acquisisce due eventi DNS, uno dal pod e l'altro dal pod del server. Ciò può generare duplicati per i seguenti esiti DNS:
 - [Backdoor:Runtime/C&CAActivity.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](#)

Gli esiti duplicati includeranno i dettagli del pod, del container e del processo che corrispondono al pod del server DNS. Puoi impostare una regola di eliminazione per eliminare gli esiti duplicati utilizzando questi campi. Il primo criterio di filtro deve utilizzare il campo Tipo di risultato con valore uguale a un tipo di esito DNS dall'elenco degli esiti fornito in precedenza in questa sezione. Il secondo criterio di filtro può essere Percorso eseguibile con valore uguale a quello del `executablePath` del server DNS o SHA-256 eseguibile con valore uguale a quello del `executableSHA256` del server DNS nell'esito generato. Come terzo criterio di filtro facoltativo, puoi utilizzare il campo Immagine del container di Kubernetes con valore uguale all'immagine del container del pod del server DNS nell'esito generato.

Creazione di regole di soppressione in GuardDuty

Una regola di soppressione è un insieme di criteri che include l'utilizzo di attributi di filtro e la fornitura di valori per i quali non si desidera GuardDuty generare un tipo di ricerca. I tipi di ricerca che soddisfano questi criteri vengono archiviati automaticamente. Per ridurre il rumore, i risultati soppressi non vengono inviati a nessuno dei dispositivi Servizi AWS con cui è possibile integrarli. Per ulteriori informazioni sui casi d'uso comuni per la creazione di regole di soppressione, vedere. [Regole di eliminazione](#)

È possibile visualizzare, creare e gestire le regole di soppressione utilizzando la pagina Regole di soppressione nella console. GuardDuty Le regole di soppressione possono essere generate anche dai filtri salvati esistenti. Per ulteriori informazioni sulla creazione dei filtri, consulta [Filtrare i risultati in GuardDuty](#).

I criteri di filtro possono includere una corrispondenza esatta utilizzando Equals e NotEquals operatori, una corrispondenza con caratteri jolly utilizzando Matches e NotMatches operatori o una corrispondenza di confronto utilizzando GreaterThan gli operatori e. GreaterThanEqualsLessThanLessThanEquals Ulteriori informazioni sugli operatori disponibili sono disponibili nella pagina. [Conditions](#)

Scegliete il metodo di accesso preferito per creare una regola di soppressione per la GuardDuty ricerca dei tipi.

Console

Per creare una regola di soppressione utilizzando la console:

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nella pagina Regole di soppressione, fai clic su Crea regola di soppressione per aprire il modulo Crea regola di soppressione.
3. Inserite un nome per la regola di soppressione. Il nome deve contenere da 3 a 64 caratteri. I caratteri validi sono A-Z, a-z, 0-9, trattino (-), trattino basso (_) e punto (.).
4. La descrizione è facoltativa. Se si immette una descrizione, questa può contenere fino a 512 caratteri. I caratteri validi sono a-z, A-Z, 0-9, punto (.), trattino (-), due punti (:), parentesi ({}()) [], barra (/) e spazio.
5. Il rango è facoltativo. Può essere un valore numerico compreso tra 1 e il conteggio totale dei filtri e delle regole di soppressione, più 1.
6. Nella sezione Attributi, selezionate una chiave e un operatore dal menu a discesa.
7. Inserisci il valore «string» o «date» dal datepicker in base alla chiave selezionata. Se è un valore di stringa, digita il testo e premi invio. È possibile aggiungere più valori in caso di valori di stringa.
8. È possibile aggiungere criteri aggiuntivi selezionando Aggiungi criteri per aggiungere un altro set di chiavi, operatori e valori.
9. Seleziona Crea regola di soppressione per creare e salvare la regola di soppressione.

Puoi anche creare una regola di eliminazione da un filtro esistente salvato. Per ulteriori informazioni sulla creazione dei filtri, consulta [Filtrare i risultati in GuardDuty](#).

Per creare una regola di eliminazione da un filtro salvato:

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guarddduty/>
2. Nella pagina Risultati, dal menu Regole salvate, seleziona una regola del set di filtri salvata. Questo mostrerà automaticamente il set di filtri e i risultati che corrispondono ai criteri.
3. Puoi anche aggiungere altri criteri di filtro a questa regola salvata. Salta questo passaggio se non sono necessari criteri di filtro aggiuntivi. Per aggiungere uno o più criteri di filtro, segui i passaggi da 3 a 7 [Adding filters on Findings page](#), quindi continua con i passaggi seguenti.
4. Dopo aver aggiunto i criteri di filtro e confermato che i risultati filtrati soddisfano i requisiti, scegli Crea regola di soppressione.
5. Inserite un nome per la regola di soppressione. Il nome deve contenere da 3 a 64 caratteri. I caratteri validi sono A-Z, a-z, 0-9, trattino (-), trattino basso (_) e punto (.).
6. La descrizione è facoltativa. Se si immette una descrizione, questa può contenere fino a 512 caratteri.
7. Scegli Create (Crea).
8. Se non è necessario aggiungere criteri di filtro aggiuntivi alla regola salvata, segui i passaggi da 4 a 7 per creare il filtro.

API/CLI

Per creare una regola di eliminazione tramite API:

1. Puoi creare regole di eliminazione tramite l'API [CreateFilter](#). Per farlo, specifica i criteri di filtro in un file JSON seguendo il formato dell'esempio riportato di seguito. L'esempio seguente sopprimerà tutti i risultati non archiviati a bassa gravità che presentano una richiesta DNS al dominio. `test.example.com` Per i risultati di gravità media, l'elenco di input sarà. `["4", "5", "7"]` Per i risultati di elevata gravità, l'elenco di input sarà `["6", "7", "8"]`. Per i risultati di gravità critica, l'elenco di input sarà `["9", "10"]`. Puoi anche applicare filtri in base a qualsiasi valore dell'elenco.

L'esempio seguente aggiunge un filtro per i risultati a bassa gravità per le funzioni lambda con il prefisso del nome della funzione "MyFunc" e il tag di funzione con prefisso diverso da "» TestTag

```
{
  "Criterion": {
    "service.action.dnsRequestAction.domain": {
      "Equals": [
        "test.example.com"
      ]
    },
    "severity": {
      "Equals": [
        "1",
        "2",
        "3"
      ]
    }
  }
}
```

È possibile creare regole di soppressione utilizzando caratteri jolly * e ? . I caratteri jolly nei filtri sono supportati solo utilizzando Matches e NotMatches operatori. Per abbinare un numero qualsiasi di caratteri, puoi usare * nel valore dell'attributo e per abbinare un singolo carattere, puoi usare ? nel valore dell'attributo. I filtri supportano un massimo di 5 attributi in una singola condizione di caratteri jolly e un massimo di 5 caratteri jolly all'interno di un singolo attributo. L'esempio seguente aggiunge un filtro per il nome Lambda che corrisponde al prefisso «MyFunc» ma non per le funzioni Lambda con tag con "TestTag" come prefisso seguito da 0-2 caratteri.

```
{
  "Criterion": {
    "resource.lambdaDetails.functionName": {
      "Matches": [
        "MyFunc*"
      ]
    },
    "resource.lambdaDetails.tags.key": {
      "NotMatches": [
        "TestTag??"
      ]
    }
  }
}
```

```
}  
  }  
}
```

Per un elenco dei nomi dei campi JSON e il relativo equivalente della console, vedere [Filtri di proprietà in GuardDuty](#).

Per testare i criteri di filtro, utilizza lo stesso criterio JSON nell'API [ListFindings](#) e conferma che siano stati selezionati gli esiti corretti. Per testare i criteri di filtro, AWS CLI segui l'esempio utilizzando il tuo detectorID e.json.

Per trovare i dati relativi detectorId al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'API [ListDetectors](#)

```
aws guardduty list-detector
```

```
aws guardduty list-findings \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--finding-criteria file://criteria.json
```

Note

Gli abbinamenti con i jolly non sono disponibili per ListFindings e GetFindingsStatistics. I criteri contenenti caratteri jolly non possono essere convalidati utilizzando e. ListFindings GetFindingsStatistics

2. Carica il filtro da utilizzare come regola di eliminazione con l'API [CreateFilter](#) o utilizzando la CLI AWS seguendo l'esempio riportato di seguito con il tuo ID rilevatore, un nome per la regola di eliminazione e il file.json.

Per trovare i dati detectorId relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#)API.


```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--action ARCHIVE \  
--name yourfiltername \  
--finding-criteria file://criteria.json
```

Puoi visualizzare un elenco dei tuoi filtri in modo programmatico con l'API [ListFilter](#). Puoi visualizzare i dettagli di un singolo filtro fornendo il nome del filtro all'API [GetFilter](#). Aggiorna i filtri utilizzando [UpdateFilter](#) o eliminali con l'API [DeleteFilter](#).

Aggiornamento delle regole di soppressione in GuardDuty

Questa sezione fornisce i passaggi per aggiornare una regola di soppressione Account AWS in uno specifico caso. Regione AWS

È possibile aggiornare le regole di soppressione esistenti dalla pagina Regole di soppressione della console. GuardDuty GuardDuty supporta l'aggiornamento della descrizione, della classificazione e dei criteri di filtro del filtro di soppressione dalla GuardDuty console o utilizzando la GuardDuty CLI/API. L'aggiornamento della regola di soppressione segue le stesse restrizioni sui valori dei campi per la descrizione, la classificazione e i criteri di. [Creazione di regole di soppressione](#)

Se sei un account membro, il tuo account amministratore può eseguire questa azione per tuo conto. Per ulteriori informazioni, consulta [Relazioni tra account amministratore e account membro](#).

Scegli il tuo metodo di accesso preferito per eliminare una regola di soppressione per GuardDuty findingtypes.

Console

1. Apri la console all' GuardDuty indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nella pagina Regole di soppressione, seleziona la regola di soppressione da aggiornare.
3. Dal menu a discesa Azioni, seleziona Aggiorna regola di soppressione.
4. Verrà aperto il modulo esistente della regola di soppressione.
5. Apportate le modifiche necessarie alla sezione Descrizione, Rango e Attributi.

6. Seleziona **Aggiorna regola di soppressione** per aggiornare la regola di soppressione.

API/CLI

Per aggiornare una regola di soppressione utilizzando l'API:

1. È possibile aggiornare le regole di soppressione tramite l' `UpdateFilter` API. Solo la descrizione, la classificazione e i criteri possono essere aggiornati utilizzando l' `UpdateFilter` API. Tutti e tre i campi sono opzionali.
2. Per aggiornare un filtro esistente, è necessario il nome del filtro che si intende aggiornare.
3. Se desideri aggiornare i criteri esistenti, crea un file JSON con i criteri aggiornati in modo simile a come hai creato il filtro per la prima volta. Un esempio di criterio per sopprimere qualsiasi risultato non archiviato a bassa gravità con una richiesta DNS al dominio `test.example.com`. Per i risultati di gravità media, l'elenco di input sarà `["4", «5", «7"]`. Per i risultati di elevata gravità, l'elenco di input sarà `["6", «7", «8"]`. Per i risultati di gravità critica, l'elenco di input sarà `["9", «10"]`. Puoi anche applicare filtri in base a qualsiasi valore dell'elenco. L'esempio seguente aggiunge un filtro per i risultati a bassa gravità.

```
{
  "Criterion": {
    "service.action.dnsRequestAction.domain": {
      "Equals": [
        "test.example.com"
      ]
    },
    "severity": {
      "Equals": [
        "1",
        "2",
        "3"
      ]
    }
  }
}
```

Per un elenco dei nomi dei campi JSON e il relativo equivalente della console, vedere [Filtri di proprietà in GuardDuty](#).

Per testare i criteri di filtro, utilizza lo stesso criterio JSON nell'API [ListFindings](#) e conferma che siano stati selezionati gli esiti corretti. Per testare i criteri di filtro, AWS CLI segui l'esempio utilizzando il tuo detectorID e.json.

Per trovare i dati relativi detectorId al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'API. [ListDetectors](#)

```
aws guardduty list-detectors --region us-east-1
```

4. Se desideri aggiornare la descrizione, puoi includere il parametro description nella chiamata CLI.
5. Se desideri aggiornare il rank, puoi includere il parametro rank nella chiamata CLI.
6. Se desideri eseguire l'aggiornamento da un filtro di soppressione a un filtro normale, utilizza il parametro action e il valore come ARCHIVE nella chiamata CLI.
7. Aggiorna l'API di filtro esistente o utilizza l'esempio AWS CLI seguente con il tuo ID del rilevatore, un nome per la regola di soppressione e il file.json.
8. Di seguito è riportato un esempio di CLI che aggiorna tutti i parametri sopra descritti. È possibile selezionare i parametri specifici da aggiornare per il proprio caso d'uso dal comando -

```
aws guardduty update-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--action ARCHIVE \  
--rank 1 \  
--description "Updated description" \  
--finding-criteria file://criteria.json
```

Eliminazione delle regole di soppressione in GuardDuty

Questa sezione fornisce i passaggi per eliminare una regola di soppressione in uno specifico Account AWS . Regione AWS

Potresti voler eliminare una regola di soppressione che non rappresenta più un comportamento previsto nel tuo ambiente. Non si desidera più sopprimere il tipo di risultato associato in modo da GuardDuty poter generare un tipo di risultato.

Se sei un account membro, il tuo account amministratore può eseguire questa azione per tuo conto. Per ulteriori informazioni, consulta [Relazioni tra account amministratore e account membro](#).

Scegli il metodo di accesso preferito per eliminare una regola di soppressione per la GuardDuty ricerca dei tipi.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nella pagina Regole di soppressione, seleziona la regola di soppressione da eliminare.
3. Dal menu a discesa Azioni, seleziona Elimina regola di soppressione.
4. Richiede un pop-up di conferma. Seleziona Elimina per procedere con l'eliminazione. Oppure seleziona Annulla per annullare l'operazione.

API/CLI

Eseguire l'API [DeleteFilter](#). Specificate il nome del filtro e l'ID del rilevatore associato per la regione specifica.

In alternativa, è possibile utilizzare il seguente AWS CLI esempio sostituendo i valori formattati in: *red*

```
aws guardduty delete-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--filter-name filterName \  
--region us-east-1
```

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Personalizzazione del rilevamento delle minacce con elenchi di entità e elenchi di indirizzi IP

Amazon GuardDuty monitora la sicurezza del tuo AWS ambiente analizzando ed elaborando i log di flusso VPC, i log degli AWS CloudTrail eventi e i log DNS. Abilitando uno o più [piani di GuardDuty protezione incentrati sui casi d'uso](#) (ad eccezione [Monitoraggio del runtime](#) di, puoi espandere le funzionalità di monitoraggio all'interno di essi). GuardDuty

Grazie agli elenchi, GuardDuty consente di personalizzare l'ambito del rilevamento delle minacce nel proprio ambiente. È possibile GuardDuty eseguire la configurazione in modo da interrompere la generazione di risultati da fonti attendibili e generare risultati per fonti dannose note dai propri elenchi di minacce. GuardDuty continua a supportare gli elenchi di indirizzi IP precedenti ed estende il supporto agli elenchi di entità (consigliato) che possono contenere indirizzi IP, domini o entrambi.

Argomenti

- [Comprendere gli elenchi di entità e gli elenchi di indirizzi IP](#)
- [Considerazioni importanti per gli elenchi GuardDuty](#)
- [Formati di elenco](#)
- [Comprensione degli stati degli elenchi](#)
- [Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP](#)
- [Aggiungere e attivare un elenco di entità o un elenco di IP](#)
- [Aggiornamento di un elenco di entità o di indirizzi IP](#)
- [Disattivazione dell'elenco di entità o dell'elenco di indirizzi IP](#)
- [Eliminazione dell'elenco di entità o dell'elenco di indirizzi IP](#)

Comprendere gli elenchi di entità e gli elenchi di indirizzi IP

GuardDuty offre due approcci di implementazione: elenchi di entità (consigliati) ed elenchi IP. Entrambi gli approcci consentono di specificare fonti attendibili, che GuardDuty impediscono di generare risultati, e minacce note, che GuardDuty utilizzano per generare risultati.

Gli elenchi di entità supportano sia gli indirizzi IP che i nomi di dominio. Utilizzano l'accesso diretto ad Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) con un'unica autorizzazione IAM che non influisce sui limiti di dimensione delle policy IAM in più regioni.

Gli elenchi IP supportano solo gli indirizzi IP e l'uso [GuardDuty ruolo collegato al servizio \(SLR\)](#) (SLR) e richiedono aggiornamenti delle policy IAM per regione, il che può influire sui limiti di dimensione delle policy IAM.

Gli elenchi attendibili (sia elenchi di entità che elenchi di indirizzi IP) includono voci ritenute affidabili per comunicazioni sicure con la propria AWS infrastruttura. GuardDuty non genera risultati per le voci elencate in fonti attendibili. In qualsiasi momento, puoi aggiungere solo un elenco di entità attendibili e un elenco di indirizzi IP attendibili Account AWS per regione.

Gli elenchi di minacce (sia gli elenchi di entità che gli elenchi di indirizzi IP) includono voci che hai identificato come fonti dannose note. Quando GuardDuty rileva un'attività che coinvolge queste fonti, genera risultati per avvisare l'utente di potenziali problemi di sicurezza. È possibile creare elenchi di minacce personalizzati o incorporare feed di intelligence sulle minacce di terze parti. Questo elenco può essere fornito dall'intelligence sulle minacce di terze parti o creato appositamente per l'organizzazione. Oltre a generare risultati a causa di un'attività potenzialmente sospetta, genera GuardDuty anche risultati basati su un'attività che coinvolge voci presenti negli elenchi delle minacce. In qualsiasi momento, puoi caricare fino a sei elenchi di entità minacciose e elenchi di indirizzi IP delle minacce Account AWS per regione.

Note

Per migrare dagli elenchi di indirizzi IP agli elenchi di entità, segui [Prerequisiti per gli elenchi di entità](#), quindi aggiungi e attiva l'elenco di entità richiesto. Dopodiché, puoi scegliere di disattivare o eliminare l'elenco di indirizzi IP corrispondente.

Considerazioni importanti per gli elenchi GuardDuty

Prima di iniziare a lavorare con gli elenchi, leggi le seguenti considerazioni:

- Gli elenchi di indirizzi IP e gli elenchi di entità si applicano solo al traffico destinato a domini e indirizzi IP instradabili pubblicamente.
- In un elenco di entità, le voci si riferiscono ai CloudTrail risultati dei log di flusso VPC in Amazon VPC e ai risultati dei log delle query DNS di Route53 Resolver.

In un elenco di indirizzi IP, le voci si applicano ai CloudTrail log di flusso VPC nei risultati di Amazon VPC, ma non ai risultati dei log delle query DNS di Route53 Resolver.

- Se includi lo stesso indirizzo IP o dominio sia negli elenchi di siti attendibili che in quelli di minacce, questa voce nell'elenco delle persone attendibili avrà la precedenza. GuardDuty non genererà alcun risultato se esiste un'attività associata a questa voce.
- In un ambiente con più account, solo l'account GuardDuty amministratore può gestire gli elenchi. Questa impostazione si applica automaticamente agli account dei membri. GuardDuty genera risultati basati su un'attività che coinvolge indirizzi IP (e domini) dannosi noti provenienti dalle fonti di minaccia dell'account amministratore e non genera risultati basati su attività che coinvolgono indirizzi IP (e domini) provenienti da fonti attendibili dell'account amministratore. Per ulteriori informazioni, consulta [Account multipli in Amazon GuardDuty](#).
- Sono accettati solo IPv4 gli indirizzi. IPv6 gli indirizzi non sono supportati.
- Dopo aver attivato, disattivato o eliminato un elenco di entità o un elenco di indirizzi IP, il processo dovrebbe essere completato entro 15 minuti. In alcuni scenari, il completamento di questo processo potrebbe richiedere fino a 40 minuti.
- GuardDuty utilizza un elenco per il rilevamento delle minacce solo quando lo stato dell'elenco diventa Attivo.
- Ogni volta che aggiungi o aggiorni una voce nella posizione del bucket S3 dell'elenco, devi attivare nuovamente l'elenco. Per ulteriori informazioni, consulta [Aggiornamento di un elenco di entità o di indirizzi IP](#).
- Gli elenchi di entità e gli indirizzi IP hanno quote diverse. Per ulteriori informazioni, consulta [GuardDuty quote](#).

Formati di elenco

GuardDuty accetta più formati di file per gli elenchi e gli elenchi di entità, con un massimo di 35 MB per file. Ogni formato presenta requisiti e funzionalità specifici.

Testo normale (TXT)

Questo formato supporta indirizzi IP, intervalli CIDR e nomi di dominio. Ogni voce deve apparire su una riga distinta.

Example Esempio di elenco di entità

```
192.0.2.1
```

```
192.0.2.0/24
example.com
example.org
*.example.org
```

Example Esempio di elenco di indirizzi IP

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

Structured Threat Information Expression (STIX)

Questo formato supporta indirizzi IP, blocchi CIDR e nomi di dominio. STIX ti consente di includere un contesto aggiuntivo nella tua intelligence sulle minacce. GuardDuty elabora indirizzi IP, intervalli CIDR e nomi di dominio a partire dagli indicatori STIX.

Example Esempio di elenco di entità

```
<?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>

```

Example Esempio di elenco di indirizzi 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

Questo formato supporta blocchi CIDR, singoli indirizzi IP e domini. Questo formato di file ha valori separati da virgole.

Example Esempio di elenco di entità

```

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

```

Example Esempio di elenco di indirizzi IP

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

FireEye™ iSight Threat Intelligence CSV

Questo formato supporta blocchi CIDR, indirizzi IP individuali e domini. I seguenti elenchi di esempio utilizzano un FireEye™ formato CSV.

Example Esemplio di elenco di entità

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdIdentifier, 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
```

```
01-00000001, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000001, https://www.example.com/  
report/01-00000001, , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,  
Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,  
1494944400
```

```
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
```

Example Esempio di elenco di indirizzi IP

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdIdentifier, 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
```

```
01-00000001, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000001, https://www.example.com/  
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,  
Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,  
1494944400
```

```
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-7bcb-40bc-a080-75bd35a2572d, , ,  
1494944400
```

Proofpoint™ ET Intelligence Feed CSV

In formato ProofPoint CSV, puoi aggiungere indirizzi IP o nomi di dominio in un unico elenco. Il seguente elenco di esempio utilizza il formato Proofpoint CSV. L'indicazione del valore per il `ports` parametro è facoltativa. Se non lo fornisci, lascia una virgola finale (,) alla fine.

Example Esempio di elenco di entità

```
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
```

Example Esempio di elenco di indirizzi 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
```

AlienVaultFeed di reputazione TM

Il seguente elenco di esempio utilizza il formato AlienVault.

Example Esempio di elenco di entità

```
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
```

Example Esempio di elenco di indirizzi 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
```

Comprensione degli stati degli elenchi

Quando aggiungi un elenco di entità o un elenco di indirizzi IP, GuardDuty mostra lo stato di tale elenco. La colonna Stato indica se l'elenco è efficace e se è necessaria un'azione. L'elenco seguente descrive i valori di stato validi:

- **Attivo:** indica che l'elenco è attualmente in uso per il rilevamento personalizzato delle minacce.
- **Inattivo:** indica che l'elenco non è attualmente in uso. GuardDuty Per utilizzare questo elenco per il rilevamento delle minacce nel proprio ambiente, vedere [Passaggio 3: Attivazione di un elenco di entità o di un elenco di indirizzi IP](#) in [Aggiungere e attivare un elenco di entità o un elenco di IP](#).
- **Errore:** indica che c'è un problema con l'elenco. Passa il mouse sullo stato per visualizzare i dettagli dell'errore.
- **Attivazione:** indica che GuardDuty è stato avviato il processo di attivazione dell'elenco. È possibile continuare a monitorare lo stato di questo elenco. Se non si verifica alcun errore, lo stato dovrebbe essere aggiornato su Attivo. Finché lo stato rimane Attivato, non è possibile eseguire alcuna azione.

in questo elenco. Potrebbero essere necessari alcuni minuti prima che lo stato dell'elenco passi ad Attivo.

- **Disattivazione:** indica che GuardDuty è stato avviato il processo di disattivazione dell'elenco. È possibile continuare a monitorare lo stato di questo elenco. Se non si verifica alcun errore, lo stato dovrebbe passare a Inattivo. Finché lo stato rimane Disattivato, non è possibile eseguire alcuna azione in questo elenco.
- **Eliminazione in sospeso:** indica che l'elenco è in fase di eliminazione. Sebbene lo stato rimanga Elimina in sospeso, non è possibile eseguire alcuna azione su questo elenco.

Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP

GuardDuty utilizza elenchi di entità ed elenchi di indirizzi IP per personalizzare il rilevamento delle minacce nell' AWS ambiente. Gli elenchi di entità (consigliato) supportano sia gli indirizzi IP che i nomi di dominio, mentre gli elenchi di indirizzi IP supportano solo gli indirizzi IP. Prima di iniziare a creare questi elenchi, è necessario aggiungere le autorizzazioni necessarie per il tipo di elenco che si desidera utilizzare.

Prerequisiti per gli elenchi di entità

Quando aggiungi elenchi di entità, GuardDuty legge gli elenchi di informazioni attendibili e sulle minacce dai bucket S3. Il ruolo che usi per creare elenchi di entità deve avere `s3:GetObject` autorizzazione perché i bucket S3 contengano questi elenchi.

Note

In un ambiente con più account, solo l'account GuardDuty amministratore può gestire gli elenchi, che si applicano automaticamente agli account dei membri.

Se non disponi già dell'`s3:GetObject` autorizzazione per la posizione del bucket S3, utilizza la seguente politica di esempio e sostituiscila *amzn-s3-demo-bucket* con la posizione del bucket S3.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
      }
    ]
  }
}

```

Prerequisiti per gli elenchi di indirizzi IP

Diverse identità IAM richiedono autorizzazioni speciali per utilizzare elenchi di IP affidabili e elenchi di minacce in GuardDuty. Un'identità con la policy gestita [AmazonGuardDutyFullAccess_v2 \(consigliato\)](#) collegata può rinominare e disattivare soltanto gli elenchi di indirizzi IP affidabili e gli elenchi minacce caricati.

Per concedere a varie identità l'accesso completo alla gestione degli elenchi di indirizzi IP affidabili e gli elenchi minacce (in aggiunta alla ridenominazione e alla disattivazione, sono inclusi anche l'aggiunta, l'attivazione, l'eliminazione e l'aggiornamento della posizione o del nome degli elenchi), assicurati che le operazioni seguenti siano presenti nella policy di autorizzazioni collegata a un utente, gruppo o ruolo:

```

{
  "Effect": "Allow",
  "Action": [
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam::555555555555:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}

```

Important

Queste operazioni non sono incluse nella policy gestita AmazonGuardDutyFullAccess.

Utilizzo della crittografia SSE-KMS con elenchi di entità ed elenchi IP

GuardDuty supporta la crittografia SSE AES256 e SSE-KMS per i tuoi elenchi. SSE-C non è supportato. Per ulteriori informazioni sui tipi di crittografia per S3, consulta [Protezione](#) dei dati mediante la crittografia lato server.

Indipendentemente dal fatto che utilizzi elenchi di entità o elenchi di IP, se utilizzi SSE-KMS, aggiungi la seguente dichiarazione alla tua politica. AWS KMS key **123456789012** Sostituiscilo con il tuo ID account.

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

Aggiungere e attivare un elenco di entità o un elenco di IP

Gli elenchi di entità e gli elenchi di indirizzi IP consentono di personalizzare le funzionalità di rilevamento delle minacce in GuardDuty. Per ulteriori informazioni su questi elenchi, vedere [Comprendere gli elenchi di entità e gli elenchi di indirizzi IP](#). Per gestire i dati affidabili e di intelligence sulle minacce per il proprio AWS ambiente, GuardDuty consiglia di utilizzare gli elenchi di entità. Prima di iniziare, consulta [Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP](#).

Scegli uno dei seguenti metodi di accesso per aggiungere e attivare un elenco di entità attendibili, un elenco di entità minacciate, un elenco di IP affidabili o un elenco di IP di minacce.

Console

(Facoltativo) fase 1: recupero dell'URL della posizione dell'elenco

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il nome del bucket Amazon S3 che contiene l'elenco specifico che vuoi aggiungere.

4. Scegli il nome dell'oggetto (elenco) per visualizzarne i dettagli.
5. Nella scheda Proprietà, copia l'URI S3 per questo oggetto.

Fase 2: aggiunta di dati affidabili o di intelligence sulle minacce

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Elenchi, scegli la scheda Elenchi di entità o Elenchi di indirizzi IP.
4. In base alla scheda selezionata, scegli di aggiungere un elenco attendibile o un elenco di minacce.
5. Nella finestra di dialogo per aggiungere un elenco di siti attendibili o di minacce, procedi nel seguente modo:
 - a. Per Nome elenco, inserisci un nome per l'elenco.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

Per un elenco di indirizzi IP, il nome dell'elenco deve essere univoco all'interno di una regione and. Account AWS

- b. Per Posizione, fornisci la posizione in cui hai caricato l'elenco. Se non hai ancora una posizione, consulta [Step 1: Fetching location URL of your list](#).

Si applica solo alle minacce personalizzate e ai set di entità affidabili personalizzati: se fornisci un URL di posizione che non corrisponde ai seguenti formati supportati, riceverai un messaggio di errore durante l'aggiunta e l'attivazione dell'elenco.

Formato dell'URL della posizione:

- <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. (Facoltativo) Per Expected bucket owner, puoi inserire l' Account AWS ID che possiede il bucket Amazon S3 specificato nel campo Posizione.

Quando non specifichi un proprietario dell' Account AWS ID, GuardDuty si comporta in modo diverso per gli elenchi di entità e gli elenchi di indirizzi IP. Per gli elenchi di entità, GuardDuty verificherà che l'account membro corrente possieda il bucket S3 specificato nel campo Posizione. Per gli elenchi di indirizzi IP, se non specifichi un proprietario dell' Account AWS ID, GuardDuty non esegue alcuna convalida.

Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione dell'elenco.

- d. Selezionare la casella di controllo I agree (Accetto).
- e. Scegliere Add list (Aggiungi elenco). Per impostazione predefinita, lo Stato dell'elenco aggiunto è Inattivo. Affinché l'elenco sia efficace, è necessario attivarlo.

Passaggio 3: attivazione di un elenco di entità o un elenco di indirizzi IP

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Elenchi, seleziona la scheda in cui desideri attivare l'elenco: Elenchi di entità o elenchi di indirizzi IP.
4. Seleziona un elenco che desideri attivare. Ciò abiliterà il menu Azione e modifica.
5. Scegli Azione, quindi scegli Attiva.

API/CLI

Per aggiungere e attivare un elenco di entità attendibili

1. Esegui [CreateTrustedEntitySet](#). Assicurati detectorId di fornire l'account membro per il quale desideri creare questo elenco di entità attendibili. Per trovare l'detectorId indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

2. In alternativa, è possibile eseguire questa operazione eseguendo il comando seguente: AWS Command Line Interface

```
aws guardduty create-trusted-entity-set \
```

```
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--format TXT \  
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-  
FILE.format" \  
--activate
```

Sostituiscilo `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco delle entità attendibili e altri valori segnaposto simili. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. `--activate --no-activate`

Il parametro `expected-bucket-owner` è facoltativo. Indipendentemente dal fatto che tu specifichi o meno il valore per questo parametro GuardDuty, verifica che l' Account AWS ID associato a questo `--detector-id` valore possieda il bucket S3 specificato nel parametro. `--location` Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Si applica solo alle minacce personalizzate e ai set di entità affidabili personalizzati: se fornisci un URL di posizione che non corrisponde ai seguenti formati supportati, riceverai un messaggio di errore durante l'aggiunta e l'attivazione dell'elenco.

Per aggiungere e attivare elenchi di entità minacciose

1. Esegui [CreateThreatEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri creare questo elenco di entità minacciose. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

2. In alternativa, è possibile eseguire questa operazione eseguendo il comando seguente: AWS Command Line Interface

```
aws guardduty create-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--format TXT \  

```

```
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

Sostituisci `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco delle entità attendibili e altri valori segnaposto simili. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. `--activate --no-activate`

Il parametro `expected-bucket-owner` è facoltativo. Indipendentemente dal fatto che tu specifichi o meno il valore per questo parametro GuardDuty, verifica che l'Account AWS ID associato a questo `--detector-id` valore possieda il bucket S3 specificato nel parametro. `--location` Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Si applica solo alle minacce personalizzate e ai set di entità affidabili personalizzati: se fornisci un URL di posizione che non corrisponde ai seguenti formati supportati, riceverai un messaggio di errore durante l'aggiunta e l'attivazione dell'elenco.

Per aggiungere e attivare un elenco di indirizzi IP attendibili

1. Esegui [Create IPSet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri creare questo elenco di indirizzi IP affidabili. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Per un elenco di indirizzi IP, il nome dell'elenco deve essere univoco all'interno di una regione Account AWS and.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

2. In alternativa, puoi farlo eseguendo il AWS Command Line Interface comando seguente e assicurati di sostituirlo `detector-id` con l'ID del rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

```
aws guardduty create-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
```

```
--format TXT \  
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-  
FILE.format" \  
--activate
```

Sostituisci `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco di IP affidabili e altri valori segnaposto simili. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. `--activate --no-activate`

Il parametro `expected-bucket-owner` è facoltativo. Quando non specifichi l'ID dell'account proprietario del bucket S3, GuardDuty non esegue alcuna convalida. Quando specifichi l'ID dell'account per il `expected-bucket-owner` parametro, GuardDuty verifica che tale Account AWS ID sia proprietario del bucket S3 specificato nel parametro. `--location` Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Per aggiungere e attivare elenchi di indirizzi IP delle minacce

1. Esegui [CreateThreatIntelSet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri creare questo elenco di indirizzi IP delle minacce. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

Per un elenco di indirizzi IP, il nome dell'elenco deve essere univoco all'interno di una regione and. Account AWS

2. In alternativa, puoi farlo eseguendo il AWS Command Line Interface comando seguente e assicurati di sostituirlo `detector-id` con l'ID del rilevatore dell'account membro per il quale aggiornerai l'elenco degli IP delle minacce.

```
aws guardduty create-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--format TXT \  

```

```
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-  
FILE.format" \  
--activate
```

Sostituisci `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco degli IP delle minacce e altri valori segnaposto simili. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. `--activate --no-activate`

Il parametro `expected-bucket-owner` è facoltativo. Quando non specifichi l'ID dell'account proprietario del bucket S3, GuardDuty non esegue alcuna convalida. Quando specifichi l'ID dell'account per il `expected-bucket-owner` parametro, GuardDuty verifica che tale Account AWS ID sia proprietario del bucket S3 specificato nel parametro. `--location` Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Dopo aver attivato un elenco di entità o un elenco di indirizzi IP, potrebbero essere necessari alcuni minuti prima che questo elenco sia efficace. Per ulteriori informazioni, consulta [Considerazioni importanti per gli elenchi GuardDuty](#).

Aggiornamento di un elenco di entità o di indirizzi IP

Gli elenchi di entità e gli elenchi di indirizzi IP consentono di personalizzare le funzionalità di rilevamento delle minacce in GuardDuty. Per ulteriori informazioni su questi elenchi, vedere [Comprendere gli elenchi di entità e gli elenchi di indirizzi IP](#).

Puoi aggiornare il nome di un elenco, la posizione del bucket S3, l'ID dell'account proprietario del bucket previsto e le voci in un elenco esistente. Se aggiorni le voci di un elenco, devi seguire i passaggi per riattivare l'elenco per GuardDuty utilizzare la versione più recente dell'elenco. Dopo aver aggiornato o attivato un elenco di entità o un elenco di indirizzi IP, potrebbero essere necessari alcuni minuti prima che questo elenco diventi effettivo. Per ulteriori informazioni, consulta [Considerazioni importanti per gli elenchi GuardDuty](#).

 Note

Se lo stato di un elenco è Attivazione, Disattivazione o Eliminazione in sospeso, devi attendere qualche minuto prima di eseguire qualsiasi azione. Per informazioni su questi stati, vedere. [Comprensione degli stati degli elenchi](#)

Scegli uno dei metodi di accesso per aggiornare un elenco di entità o un elenco di indirizzi IP.

Console

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Elenchi, seleziona la scheda appropriata: Elenchi di entità o elenchi di indirizzi IP.
4. Seleziona un elenco (attendibile o pericoloso) che desideri aggiornare. Ciò abiliterà il menu Azione e Modifica.
5. Scegli Modifica.
6. Nella finestra di dialogo per aggiornare l'elenco, specifica i dettagli che desideri aggiornare.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

Per un elenco di indirizzi IP, il nome dell'elenco deve essere univoco all'interno di una regione and. Account AWS

Si applica solo alle minacce personalizzate e ai set di entità affidabili personalizzati: se fornisci un URL di posizione che non corrisponde ai seguenti formati supportati, riceverai un messaggio di errore durante l'aggiunta e l'attivazione dell'elenco.

7. (Facoltativo) Per Expected bucket owner, puoi inserire l' Account AWS ID che possiede il bucket Amazon S3 specificato nel campo Posizione.

Quando non specifichi un Account AWS ID proprietario, GuardDuty si comporta in modo diverso per gli elenchi di entità e gli elenchi di indirizzi IP. Per gli elenchi di entità, GuardDuty verificherà che l'account membro corrente possieda il bucket S3 specificato nel campo

Posizione. Per gli elenchi di indirizzi IP, se non specifichi un proprietario dell' Account AWS ID, GuardDuty non esegue alcuna convalida.

Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione dell'elenco.

8. Seleziona la casella di controllo Accetto, quindi scegli Aggiorna elenco.

API/CLI

Per iniziare con le seguenti procedure, è necessario l'ID, ad esempio `trustedEntitySetId` `threatEntitySetId` `trustedIpSet`, `othreatIpSet`, associato alla risorsa dell'elenco che si desidera aggiornare.

Per aggiornare e attivare un elenco di entità attendibili

1. Esegui [UpdateTrustedEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri aggiornare questo elenco di entità attendibili. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando che aggiorna l'elenco e attiva anche questo elenco: `name`

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

Sostituiscilo `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco delle entità attendibili e altri valori segnaposto simili. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. `--activate --no-activate`

Il parametro `expected-bucket-owner` è facoltativo. Indipendentemente dal fatto che tu specifichi o meno il valore per questo parametro GuardDuty, verifica che l' Account AWS ID associato a questo `--detector-id` valore possieda il bucket S3 specificato nel parametro. `--location` Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Si applica solo alle minacce personalizzate e ai set di entità affidabili personalizzati: se fornisci un URL di posizione che non corrisponde ai seguenti formati supportati, riceverai un messaggio di errore durante l'aggiunta e l'attivazione dell'elenco.

Per aggiornare e attivare un elenco di entità minacciose

1. Esegui [UpdateThreatEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri creare questo elenco di entità minacciose. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando che aggiorna l'elenco e attiva anche questo elenco: `name`

```
aws guardduty update-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--threat-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

Sostituiscilo `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco delle entità minacciose e altri valori segnato simili. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. `--activate --no-activate`

Il parametro `expected-bucket-owner` è facoltativo. Indipendentemente dal fatto che tu specifichi o meno il valore per questo parametro GuardDuty, verifica che l' Account AWS ID associato a questo `--detector-id` valore possieda il bucket S3 specificato nel parametro.

--location Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Si applica solo alle minacce personalizzate e ai set di entità affidabili personalizzati: se fornisci un URL di posizione che non corrisponde ai seguenti formati supportati, riceverai un messaggio di errore durante l'aggiunta e l'attivazione dell'elenco.

Per aggiornare e attivare un elenco di indirizzi IP affidabili

1. Esegui [Create IPSet](#). Assicurati detectorId di fornire l'account membro per il quale desideri aggiornare questo elenco di indirizzi IP affidabili. Per trovare l'detectorId indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

Per un elenco di indirizzi IP, il nome dell'elenco deve essere univoco all'interno di una regione and. Account AWS

2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando che attiva anche l'elenco:

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

Sostituisci detector-id con l'ID del rilevatore dell'account membro per il quale aggiornerai l'elenco degli IP affidabili e altri valori segnaposto corrispondenti. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. --activate --no-activate

Il parametro expected-bucket-owner è facoltativo. Quando non specifichi l'ID dell'account proprietario del bucket S3, GuardDuty non esegue alcuna convalida. Quando specifichi l'ID dell'account per il expected-bucket-owner parametro, GuardDuty verifica che tale Account AWS ID sia proprietario del bucket S3 specificato nel parametro. --location Se

GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Per aggiungere e attivare elenchi di indirizzi IP delle minacce

1. Esegui [CreateThreatIntelSet](#). Assicurati detectorId di fornire l'account membro per il quale desideri creare questo elenco di indirizzi IP delle minacce. Per trovare l'detectorId indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

Per un elenco di indirizzi IP, il nome dell'elenco deve essere univoco all'interno di una regione and. Account AWS

2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando che attiva anche l'elenco:

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

Sostituiscilo detector-id con l'ID del rilevatore dell'account membro per il quale aggiornerai l'elenco degli IP delle minacce e altri valori segnato corrispondenti. *shown in red*

Se non desideri attivare questo elenco appena creato, sostituisci il parametro con. --activate --no-activate

Il parametro expected-bucket-owner è facoltativo. Quando non specifichi l'ID dell'account proprietario del bucket S3, GuardDuty non esegue alcuna convalida. Quando specifichi l'ID dell'account per il expected-bucket-owner parametro, GuardDuty verifica che tale Account AWS ID sia proprietario del bucket S3 specificato nel parametro. --location Se GuardDuty rileva che questo bucket S3 non appartiene all'ID account specificato, riceverai un errore al momento dell'attivazione di questo elenco.

Disattivazione dell'elenco di entità o dell'elenco di indirizzi IP

Quando non desideri più GuardDuty utilizzare un elenco, puoi disattivarlo. Il completamento del processo potrebbe richiedere alcuni minuti. Per ulteriori informazioni, consulta [Considerazioni importanti per gli elenchi GuardDuty](#). Dopo la disattivazione dell'elenco, le voci nell'elenco delle entità o nell'elenco degli indirizzi IP non influiranno sul rilevamento delle minacce in GuardDuty.

Scegli uno dei metodi di accesso per disattivare l'elenco.

Console

Per disattivare l'elenco delle entità o l'elenco degli indirizzi IP

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Elenco, seleziona la scheda in cui desideri disattivare l'elenco: Elenchi di entità o Elenco di indirizzi IP.
4. Nella scheda selezionata, seleziona l'elenco che desideri disattivare.
5. Scegli Azioni, quindi scegli Disattiva.
6. Conferma l'azione e scegli Disattiva.

API/CLI

Per iniziare con le seguenti procedure, è necessario l'ID, ad esempio `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet`, `othreatIpSet`, associato alla risorsa dell'elenco che desideri disattivare.

Per disattivare un elenco di entità attendibili

1. Esegui [UpdateTrustedEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri disattivare questo elenco di entità fidate. Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando:

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
```

```
--no-activate
```

Sostituisci `detector-id` con l'ID del rilevatore dell'account membro per il quale disattiverai l'elenco delle entità attendibili e gli altri valori segnaposto corrispondenti. *shown in red*

Per disattivare gli elenchi di entità minacciate

1. Esegui [UpdateThreatEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri disattivare questo elenco di entità minacciose. Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando:

```
aws guardduty update-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Sostituisci `detector-id` con l'ID del rilevatore dell'account membro per il quale creerai l'elenco delle entità minacciose e altri valori segnaposto simili. *shown in red*

Per disattivare un elenco di indirizzi IP affidabili

1. Esegui l'[aggiornamento IPSet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri disattivare questo elenco di indirizzi IP affidabili. Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il AWS Command Line Interface comando seguente e assicurati di sostituirlo `detector-id` con l'ID del rilevatore dell'account membro per il quale disattiverai l'elenco di indirizzi IP affidabili.

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Per disattivare l'elenco degli IP delle minacce

1. Esegui [UpdateThreatIntelSet](#). Assicurati detectorId di fornire l'account membro per il quale desideri disattivare questo elenco di indirizzi IP delle minacce. Per trovare l'indirizzo detectorId per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando e assicurati di sostituirlo detector-id con l'ID del rilevatore dell'account membro per il quale disattiverai l'elenco degli IP delle minacce.

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Eliminazione dell'elenco di entità o dell'elenco di indirizzi IP

Quando non desideri più mantenere una voce dell'elenco nel set di entità o nel set di indirizzi IP, puoi eliminarla. Il completamento del processo potrebbe richiedere alcuni minuti. Per ulteriori informazioni, consulta [Considerazioni importanti per gli elenchi GuardDuty](#).

Se lo stato dell'elenco è Attivazione o Disattivazione, è necessario attendere alcuni minuti prima di eseguire qualsiasi azione. Per ulteriori informazioni, consulta [Comprensione degli stati degli elenchi](#).

Scegli uno dei metodi di accesso per eliminare l'elenco.

Console

Per eliminare l'elenco di entità o l'elenco di indirizzi IP

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Elenco, seleziona la scheda in cui desideri eliminare l'elenco: Elenchi di entità o Elenco di indirizzi IP.
4. Nella scheda selezionata, seleziona l'elenco che desideri eliminare.
5. Scegli Azioni, quindi Elimina.

Lo stato dell'elenco cambierà in Elimina in sospeso. L'eliminazione dell'elenco potrebbe richiedere alcuni minuti.

API/CLI

Per iniziare con le seguenti procedure, è necessario l'ID, ad esempio `trustedEntitySetId` `threatEntitySetId` `trustedIpSet`, `othreatIpSet`, associato alla risorsa dell'elenco che si desidera eliminare.

Per eliminare un elenco di entità attendibili

1. Esegui [DeleteTrustedEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri eliminare questo elenco di entità attendibili. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando:

```
aws guardduty delete-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example
```

Sostituiscilo `detector-id` con l'ID del rilevatore dell'account membro per il quale eliminerai l'elenco delle entità attendibili e gli altri valori segnaposto corrispondenti. *shown in red*

Per disattivare gli elenchi di entità minacciose

1. Esegui [DeleteThreatEntitySet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri eliminare questo elenco di entità minacciose. Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il seguente AWS Command Line Interface comando:

```
aws guardduty delete-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

Sostituiscilo `detector-id` con l'ID del rilevatore dell'account membro per il quale eliminerai l'elenco delle entità minacciose e altri valori segnaposto corrispondenti. *shown in red*

Per eliminare un elenco di indirizzi IP attendibili

1. Esegui [Elimina IPSet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri eliminare questo elenco di indirizzi IP affidabili. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il AWS Command Line Interface comando seguente e assicurati di sostituirlo `detector-id` con l'ID del rilevatore dell'account membro per il quale eliminerai l'elenco di indirizzi IP affidabili.

```
aws guardduty delete-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example
```

Sostituiscilo `detector-id` con l'ID del rilevatore dell'account membro per il quale eliminerai l'elenco delle entità minacciose e altri valori segnaposto simili. *shown in red*

Per eliminare l'elenco degli IP delle minacce

1. Esegui [DeleteThreatIntelSet](#). Assicurati `detectorId` di fornire l'account membro per il quale desideri eliminare questo elenco di indirizzi IP delle minacce. Per trovare l'`detectorId` indirizzo per il tuo account e la regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.
2. In alternativa, puoi farlo eseguendo il AWS Command Line Interface comando seguente e assicurati di sostituirlo `detector-id` con l'ID del rilevatore dell'account membro per il quale eliminerai l'elenco degli IP delle minacce.

```
aws guardduty delete-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example
```


Sostituisci `detector-id` con l'ID del rilevatore dell'account membro per il quale eliminerai l'elenco delle entità minacciose e altri valori segnaposto simili. *shown in red*

Esportazione dei GuardDuty risultati generati nei bucket Amazon S3

GuardDuty conserva i risultati generati per un periodo di 90 giorni. GuardDuty esporta i risultati attivi su Amazon EventBridge (EventBridge). Facoltativamente, puoi esportare i risultati generati in un bucket Amazon Simple Storage Service (Amazon S3). Questo ti aiuterà a tenere traccia dei dati storici delle attività potenzialmente sospette nel tuo account e a valutare se le misure correttive consigliate hanno avuto successo.

Tutti i nuovi risultati attivi GuardDuty generati vengono esportati automaticamente entro circa 5 minuti dalla generazione del risultato. È possibile impostare la frequenza con cui vengono esportati gli aggiornamenti dei risultati attivi. EventBridge La frequenza selezionata si applica all'esportazione di nuove occorrenze di risultati esistenti nel bucket S3 (se configurato) e in Detective (se integrato). EventBridge Per informazioni su come GuardDuty aggrega più occorrenze di risultati esistenti, consulta. [GuardDuty ricerca dell'aggregazione](#)

Quando configuri le impostazioni per esportare i risultati in un bucket Amazon S3, GuardDuty utilizza AWS Key Management Service (AWS KMS) per crittografare i dati dei risultati nel bucket S3. Ciò richiede l'aggiunta di autorizzazioni al bucket S3 e alla AWS KMS chiave in modo che GuardDuty possa utilizzarle per esportare i risultati nel tuo account.

Indice

- [Considerazioni](#)
- [Fase 1 — Autorizzazioni necessarie per esportare i risultati](#)
- [Fase 2: Allegare la policy alla chiave KMS](#)
- [Fase 3: Allegare la policy al bucket Amazon S3](#)
- [Fase 4 - Esportazione dei risultati in un bucket S3 \(console\)](#)
- [Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati](#)

Considerazioni

Prima di procedere con i prerequisiti e i passaggi per esportare i risultati, considera i seguenti concetti chiave:

- Le impostazioni di esportazione sono regionali: è necessario configurare le opzioni di esportazione in ogni regione in cui si utilizza GuardDuty
- Esportazione dei risultati in bucket Amazon S3 in Regioni AWS diverse aree geografiche
GuardDuty : supporta le seguenti impostazioni di esportazione:
 - Il bucket o l'oggetto Amazon S3 e la AWS KMS chiave devono appartenere allo stesso. Regione AWS
 - Per i risultati generati in una regione commerciale, puoi scegliere di esportarli in un bucket S3 in qualsiasi regione commerciale. Tuttavia, non puoi esportare questi risultati in un bucket S3 in una regione opt-in.
 - Per i risultati generati in una regione opt-in, puoi scegliere di esportarli nella stessa regione opt-in in cui vengono generati o in qualsiasi regione commerciale. Tuttavia, non puoi esportare i risultati da una regione opt-in a un'altra regione opt-in.
- Autorizzazioni per esportare i risultati: per configurare le impostazioni per l'esportazione dei risultati attivi, il bucket S3 deve disporre delle autorizzazioni che consentano di caricare oggetti. GuardDuty È inoltre necessario disporre di una AWS KMS chiave che GuardDuty possa essere utilizzata per crittografare i risultati.
- I risultati archiviati non vengono esportati: il comportamento predefinito prevede che i risultati archiviati, incluse le nuove istanze di risultati soppressi, non vengano esportati.

Quando un GuardDuty risultato viene generato come archiviato, è necessario estrarlo dall'archivio. Ciò modifica lo stato di ricerca del filtro su Attivo. GuardDuty esporta gli aggiornamenti ai risultati non archiviati esistenti in base alla configurazione. [Fase 5 — Frequenza di esportazione dei risultati](#)

- GuardDuty l'account amministratore può esportare i risultati generati negli account membro associati: quando si configurano i risultati di esportazione in un account amministratore, tutti i risultati degli account membro associati generati nella stessa regione vengono esportati nella stessa posizione configurata per l'account amministratore. Per ulteriori informazioni, consulta [Comprensione della relazione tra account GuardDuty amministratore e account membro](#).

Fase 1 — Autorizzazioni necessarie per esportare i risultati

Quando configuri le impostazioni per l'esportazione dei risultati, selezioni un bucket Amazon S3 in cui archiviare i risultati e AWS KMS una chiave da utilizzare per la crittografia dei dati. Oltre alle GuardDuty autorizzazioni per le azioni, devi disporre anche delle autorizzazioni per le seguenti azioni per configurare correttamente le impostazioni per esportare i risultati:

- `s3:GetBucketLocation`
- `s3:PutObject`

Se devi esportare i risultati in un prefisso specifico nel tuo bucket Amazon S3, devi anche aggiungere le seguenti autorizzazioni al ruolo IAM:

- `s3:GetObject`
- `s3:ListBucket`

Fase 2: Allegare la policy alla chiave KMS

GuardDuty crittografa i dati dei risultati nel bucket utilizzando AWS Key Management Service. Per configurare correttamente le impostazioni, devi prima GuardDuty autorizzare l'uso di una chiave KMS. Puoi concedere le autorizzazioni [collegando la policy](#) alla tua chiave KMS.

Quando utilizzi una chiave KMS di un altro account, devi applicare la politica delle chiavi accedendo al proprietario della Account AWS chiave. Quando configuri le impostazioni per esportare i risultati, avrai anche bisogno della chiave ARN dell'account che possiede la chiave.

Per modificare la politica delle chiavi KMS per GuardDuty crittografare i risultati esportati

1. [Apri la AWS KMS console in /kms. https://console.aws.amazon.com](https://console.aws.amazon.com/kms)
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Seleziona una chiave KMS esistente o esegui i passaggi per [creare una nuova chiave](#) nella Guida per gli AWS Key Management Service sviluppatori, che utilizzerai per crittografare i risultati esportati.

 Note

La Regione AWS chiave KMS e il bucket Amazon S3 devono coincidere.

Puoi utilizzare lo stesso bucket S3 e la stessa key pair KMS per esportare i risultati da qualsiasi regione applicabile. Per ulteriori informazioni, consulta l'articolo sull'esportazione [Considerazioni](#) dei risultati tra regioni.

4. Nella sezione Key policy (Policy chiave), scegli Edit (Modifica).

Se è visualizzata la visualizzazione Passa alla politica, selezionala per visualizzare la Politica chiave, quindi scegli Modifica.

5. Copia il seguente blocco di policy nella tua policy chiave KMS per concedere l'GuardDuty autorizzazione all'uso della tua chiave.

```
{
  "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. Modifica la politica sostituendo i seguenti valori formattati *red* nell'esempio di policy:

1. Sostituisci *KMS key ARN* con l'Amazon Resource Name (ARN) della chiave KMS. Per individuare l'ARN della chiave, consulta [Finding the key ID and ARN](#) nella Developer Guide.AWS Key Management Service
2. *123456789012* Sostituiscilo con l' Account AWS ID proprietario dell' GuardDuty account che esporta i risultati.

3. Sostituisci *Region2* con il Regione AWS luogo in cui vengono generati i GuardDuty risultati.
4. Sostituisci *SourceDetectorID* con l' GuardDuty account detectorID della regione specifica in cui sono stati generati i risultati.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectorsAPI](#).

Note

Se lo utilizzi GuardDuty in una regione con attivazione, sostituisci il valore per «Servizio» con l'endpoint regionale per quella regione. Ad esempio, se utilizzi GuardDuty nella regione Medio Oriente (Bahrein) (me-south-1), sostituisci con. "Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com" [Per informazioni sugli endpoint per ogni regione opt-in, consulta endpoint e quote. GuardDuty](#)

7. Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la sintassi JSON della tua politica delle chiavi KMS sia valida.

Scegli Save (Salva).

8. (Facoltativo) Copia la chiave ARN su un blocco note per utilizzarla nei passaggi successivi.

Fase 3: Allegare la policy al bucket Amazon S3

Aggiungi le autorizzazioni al bucket Amazon S3 in cui esporterai i risultati in modo da poter caricare oggetti in GuardDuty questo bucket S3. Indipendentemente dall'utilizzo di un bucket Amazon S3 che appartiene al tuo account o a un altro Account AWS, devi aggiungere queste autorizzazioni.

Se in qualsiasi momento decidi di esportare i risultati in un altro bucket S3, per continuare a esportare i risultati, devi aggiungere le autorizzazioni a quel bucket S3 e configurare nuovamente le impostazioni dei risultati di esportazione.

Se non disponi già di un bucket Amazon S3 in cui esportare questi risultati, consulta [Creating a bucket](#) nella Amazon S3 User Guide.

Per allegare le autorizzazioni alla tua policy sui bucket S3

1. Esegui i passaggi indicati in [Per creare o modificare una policy sui bucket](#) nella Guida per l'utente di Amazon S3, finché non viene visualizzata la pagina Modifica policy del bucket.
2. La policy di esempio mostra come concedere GuardDuty l'autorizzazione all'esportazione dei risultati nel bucket Amazon S3. Se modifichi il percorso dopo aver configurato i risultati di esportazione, devi modificare la politica per concedere l'autorizzazione alla nuova posizione.

Copia la seguente politica di esempio e incollala nell'editor delle politiche Bucket.

Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la sintassi JSON della tua politica delle chiavi KMS sia valida.

Esempio di politica del bucket 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. Modifica la politica sostituendo i seguenti valori formattati *red* nell'esempio di policy:

1. Sostituisci *Amazon S3 bucket ARN* con l'Amazon Resource Name (ARN) del bucket Amazon S3. Puoi trovare il Bucket ARN nella pagina Modifica policy del bucket nella console. <https://console.aws.amazon.com/s3/>
2. *123456789012* Sostituiscilo con l' Account AWS ID proprietario dell' GuardDuty account che esporta i risultati.
3. Sostituisci *us-east-2* con il Regione AWS luogo in cui vengono generati i GuardDuty risultati.
4. Sostituisci *SourceDetectorID* con l' GuardDuty account detectorID della regione specifica in cui sono stati generati i risultati.

Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella <https://console.aws.amazon.com/guardduty/console> o esegui l'[ListDetectors](#) API.

5. Sostituisci *[optional prefix]* parte del valore del *S3 bucket ARN/[optional prefix]* segnaposto con una posizione di cartella opzionale in cui desideri esportare i risultati. Per ulteriori informazioni sull'uso dei prefissi, consulta [Organizing objects using prefixes](#) nella Amazon S3 User Guide.

Se fornisci una posizione opzionale per la cartella che non esiste già, la GuardDuty creerà solo se l'account associato al bucket S3 è lo stesso dell'account che esporta i risultati. Quando esporti i risultati in un bucket S3 che appartiene a un altro account, la posizione della cartella deve già esistere.

6. Sostituisci **KMS key ARN** con l'Amazon Resource Name (ARN) della chiave KMS associata alla crittografia dei risultati esportati nel bucket S3. Per individuare l'ARN della chiave, consulta [Finding the key ID and ARN](#) nella Developer Guide.AWS Key Management Service

Note

Se lo utilizzi GuardDuty in una regione con attivazione, sostituisci il valore per il «Servizio» con l'endpoint regionale per quella regione. Ad esempio, se utilizzi GuardDuty nella regione Medio Oriente (Bahrein) (me-south-1), sostituisci con. "Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com" [Per informazioni sugli endpoint per ogni regione opt-in, consulta endpoint e quote. GuardDuty](#)

4. Scegli Save (Salva).

Fase 4 - Esportazione dei risultati in un bucket S3 (console)

GuardDuty consente di esportare i risultati in un bucket esistente in un altro. Account AWS

Quando crei un nuovo bucket S3 o scegli un bucket esistente nel tuo account, puoi aggiungere un prefisso opzionale. Quando configuri i risultati dell'esportazione, GuardDuty crea una nuova cartella nel bucket S3 per i risultati. Il prefisso verrà aggiunto alla struttura di cartelle predefinita creata. GuardDuty Ad esempio, il formato del prefisso opzionale. /AWSLogs/**123456789012**/GuardDuty/**Region**

L'intero percorso dell'oggetto S3 sarà. **amzn-s3-demo-bucket/prefix-name/UUID.json.gz**
UUIDViene generato casualmente e non rappresenta l'ID del rilevatore o l'ID del ritrovamento.

Important

La chiave KMS e il bucket S3 devono trovarsi nella stessa regione.

Prima di completare questi passaggi, assicurati di aver collegato le rispettive politiche alla tua chiave KMS e al bucket S3 esistente.

Per configurare i risultati delle esportazioni

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Impostazioni, in Opzioni di esportazione di Findings, per il bucket S3, scegli Configura ora (o Modifica, se necessario).
4. Per l'ARN del bucket S3, inserisci. **bucket ARN** Per trovare l'ARN del bucket, [consulta Visualizzazione delle proprietà di un bucket S3 nella Amazon S3](#) User Guide.
5. Per l'ARN della chiave KMS, inserisci. **key ARN** Per individuare l'ARN della chiave, consulta [Finding the key ID and ARN](#) nella Developer Guide.AWS Key Management Service
6. Allega politiche
 - Esegui i passaggi per allegare la policy del bucket S3. Per ulteriori informazioni, consulta [Fase 3: Allegare la policy al bucket Amazon S3](#).
 - Esegui i passaggi per allegare la policy delle chiavi KMS. Per ulteriori informazioni, consulta [Fase 2: Allegare la policy alla chiave KMS](#).
7. Scegli Save (Salva).

Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati

Configura la frequenza di esportazione dei risultati attivi aggiornati in base al tuo ambiente. Per impostazione predefinita, i risultati aggiornati vengono esportati ogni 6 ore. Ciò significa che tutti i risultati aggiornati dopo l'esportazione più recente sono inclusi nella successiva esportazione. Se i risultati aggiornati vengono esportati ogni 6 ore e l'esportazione avviene alle 12:00, qualsiasi scoperta che si aggiorna dopo le 12:00 viene esportata alle 18:00.

Per impostare la frequenza

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Seleziona Impostazioni.

3. Nella sezione Opzioni di esportazione dei risultati, scegli Frequenza dei risultati aggiornati. Questo imposta la frequenza per l'esportazione dei risultati Active aggiornati sia EventBridge su Amazon S3 che su Amazon S3. È possibile scegliere tra le seguenti opzioni:
 - Update EventBridge e S3 ogni 15 minuti
 - Update EventBridge e S3 ogni 1 ora
 - Aggiornamento EventBridge e S3 ogni 6 ore (impostazione predefinita)
4. Scegli Save changes (Salva modifiche).

Elaborazione dei GuardDuty risultati con Amazon EventBridge

GuardDuty pubblica (invia) automaticamente i risultati come eventi ad Amazon EventBridge (precedentemente CloudWatch Amazon Events), un servizio di bus eventi senza server. EventBridge fornisce un flusso di dati quasi in tempo reale da applicazioni e servizi a destinazioni come argomenti AWS Lambda, funzioni e flussi Amazon Kinesis di Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni, consulta [Amazon EventBridge User Guide](#).

EventBridge consente il monitoraggio e l'elaborazione automatizzati dei GuardDuty risultati mediante la ricezione di [eventi](#). EventBridge riceve eventi sia per i risultati di nuova generazione che per i risultati aggregati, in cui le occorrenze successive di un risultato esistente vengono combinate con quelle originali. A ogni GuardDuty risultato viene assegnato un ID di ricerca e GuardDuty crea un EventBridge evento per ogni risultato con un ID di risultato univoco. Per informazioni su come funziona l'aggregazione GuardDuty, consulta [GuardDuty ricerca dell'aggregazione](#).

Oltre al monitoraggio e all'elaborazione automatizzati, l'utilizzo di EventBridge consente la conservazione a lungo termine dei dati relativi ai risultati. GuardDuty archivia i risultati per 90 giorni. Con EventBridge, puoi inviare i dati dei risultati alla tua piattaforma di archiviazione preferita e archivarli per tutto il tempo che desideri. Per conservare i risultati per un periodo più lungo, GuardDuty supporta [Esportazione dei risultati generati su Amazon S3](#).

Argomenti

- [Comprensione EventBridge della frequenza delle notifiche in GuardDuty](#)
- [Configura un argomento e un endpoint di Amazon SNS \(Email, Slack e Amazon Chime\)](#)
- [Utilizzo di Amazon EventBridge per GuardDuty i risultati](#)
- [Creazione di una EventBridge regola per GuardDuty i risultati](#)
- [EventBridge regola per ambienti con GuardDuty più account](#)

Comprensione EventBridge della frequenza delle notifiche in GuardDuty

Questa sezione spiega con quale frequenza si ricevono le notifiche di ricerca EventBridge e come aggiornare la frequenza delle successive occorrenze di ricerca.

Notifiche per i risultati appena generati con un ID di risultato univoco

GuardDuty invia queste notifiche quasi in tempo reale quando genera un risultato con un ID di risultato univoco. La notifica include tutte le occorrenze successive di queste occorrenze successive di questo ID di risultato durante il processo di generazione della notifica.

La frequenza di notifica per i risultati appena generati è quasi in tempo reale. Per impostazione predefinita, non è possibile modificare questa frequenza.

Notifiche per occorrenze di esiti successive

GuardDuty aggrega tutte le occorrenze successive di un particolare tipo di risultato che si verificano entro intervalli di 6 ore in un unico evento. Solo un account amministratore può aggiornare la frequenza di EventBridge notifica per le successive occorrenze di ricerca. Un account membro non può aggiornare questa frequenza per il proprio account. Ad esempio, se l'account GuardDuty amministratore delegato aggiorna la frequenza a un'ora, tutti gli account membro avranno anche una frequenza di notifica di un'ora sulle successive occorrenze di ricerca inviate. EventBridge Per ulteriori informazioni, consulta [Account multipli in Amazon GuardDuty](#).

In qualità di account amministratore, puoi personalizzare la frequenza predefinita delle notifiche sulle successive occorrenze di ricerca. I valori possibili sono 15 minuti, 1 ora o 6 ore (impostazione predefinita). Per ulteriori informazioni sull'impostazione della frequenza di queste notifiche, consulta [Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati](#).

Per ulteriori dettagli sulla ricezione di EventBridge notifiche da parte dell'account amministratore per gli account dei membri, consulta [EventBridge regola per ambienti con più account](#).

Configura un argomento e un endpoint di Amazon SNS (Email, Slack e Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) è un servizio completamente gestito che fornisce il recapito dei messaggi dagli editori agli abbonati. Gli editori comunicano in modo asincrono con gli abbonati inviando messaggi su un argomento. Un argomento è un punto di accesso logico e un

canale di comunicazione che consente di raggruppare più endpoint come AWS Lambda Amazon Simple Queue Service (Amazon SQS), HTTP/S e un indirizzo e-mail.

Note

Puoi aggiungere un argomento di Amazon SNS alla tua regola di EventBridge evento preferita durante o dopo la creazione della regola.

Crea un argomento Amazon SNS

Per iniziare, devi prima impostare un argomento in Amazon SNS e aggiungere un endpoint. Per creare un argomento, esegui i passaggi descritti nel [Passaggio 1: Creazione di un argomento](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service. Dopo aver creato l'argomento, copia l'ARN dell'argomento negli appunti. Utilizzerai questo argomento ARN per continuare con una delle configurazioni preferite.

Scegliete un metodo preferito per stabilire dove inviare i dati di GuardDuty ricerca.

Email setup

Per configurare un endpoint di posta elettronica

Dopo di te [Create an Amazon SNS topic](#), il passaggio successivo consiste nel creare un abbonamento a questo argomento. Esegui i passaggi indicati nella [Fase 2: Creazione di un abbonamento a un argomento di Amazon SNS nella Amazon Simple Notification Service Developer Guide](#).

1. Per Argomento ARN, utilizza l'argomento ARN creato nel passaggio. [Create an Amazon SNS topic](#) L'argomento ARN è simile al seguente:

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. Per Protocol (Protocollo), selezionare Email (E-mail).
3. Per Endpoint, inserisci un indirizzo e-mail a cui desideri ricevere le notifiche da Amazon SNS.

Dopo aver creato l'abbonamento, dovrai confermarlo tramite il tuo client di posta elettronica.

Slack setup

Per configurare un Amazon Q Developer nel client di applicazioni di chat: Slack

Dopo di te [Create an Amazon SNS topic](#), il passaggio successivo consiste nel configurare il client per Slack.

Esegui i passaggi indicati in [Tutorial: Inizia a usare Slack](#) nella Guida per amministratori delle applicazioni Amazon Q Developer in chat.

Chime setup

Per configurare un Amazon Q Developer nel client di applicazioni di chat - Chime

Dopo di te [Create an Amazon SNS topic](#), il passaggio successivo consiste nel configurare Amazon Q Developer for Chime.

Esegui i passaggi indicati in [Tutorial: Inizia a usare Amazon Chime](#) nella Guida per amministratori delle applicazioni Amazon Q Developer in chat.

Utilizzo di Amazon EventBridge per GuardDuty i risultati

Con EventBridge, crei regole per specificare gli eventi che desideri monitorare. Queste regole specificano anche i servizi e le applicazioni di destinazione che possono eseguire azioni automatiche se si verificano questi eventi. Una [destinazione](#) è una destinazione (una risorsa o un endpoint) che EventBridge invia un evento quando l'evento corrisponde al modello di evento definito nella regola. Ogni evento è un oggetto JSON conforme allo EventBridge schema degli AWS eventi e contiene una rappresentazione JSON di un risultato. È possibile personalizzare la regola per inviare solo gli eventi che soddisfano determinati criteri. Per ulteriori informazioni, vedere [Argomento sullo schema JSON]. Poiché i dati dei risultati sono strutturati come un [EventBridgeevento](#), è possibile monitorare, elaborare e agire in base ai risultati utilizzando altre applicazioni, servizi e strumenti.

Per ricevere notifiche sui GuardDuty risultati in base agli eventi, devi creare una EventBridge regola e un obiettivo per GuardDuty. Questa regola consente EventBridge di inviare notifiche relative ai risultati GuardDuty generati all'obiettivo specificato nella regola.

Note

EventBridge e CloudWatch gli eventi sono lo stesso servizio e la stessa API sottostanti. Tuttavia, EventBridge include funzionalità aggiuntive che consentono di ricevere eventi dalle

applicazioni SaaS (Software as a Service) e dalle proprie applicazioni. Poiché il servizio e l'API sottostanti sono gli stessi, anche lo schema degli eventi per GuardDuty i risultati è lo stesso.

In che modo funzionano i risultati archiviati e non archiviati con GuardDuty EventBridge

Per i risultati archiviati manualmente, le occorrenze iniziali e tutte le successive di tali risultati (generate dopo il completamento dell'archiviazione) vengono inviate in EventBridge base a una frequenza di notifica specifica. Per ulteriori informazioni, consulta [Comprensione EventBridge della frequenza delle notifiche in GuardDuty](#).

Per i risultati che vengono archiviati automaticamente [Regole di eliminazione](#), le occorrenze iniziali e tutte le successive di questi risultati (generate dopo il completamento dell'archiviazione) non vengono inviate a EventBridge. È possibile visualizzare questi risultati archiviati automaticamente nella console GuardDuty.

Schema degli eventi

Un [modello di evento](#) definisce i dati EventBridge utilizzati per determinare se inviare l'evento alla destinazione. L' EventBridge evento per GuardDuty ha il seguente formato:

```
{
  "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}
}
```

Il `detail` valore restituisce i dettagli JSON di un singolo risultato come oggetto, anziché restituire l'intera sintassi di risposta ai risultati che supporta più risultati all'interno di un array.

Per un elenco completo di tutti i parametri inclusi in `GUARDDUTY_FINDING_JSON_OBJECT`, vedere [GetFindings](#). Il parametro `id` visualizzato in `GUARDDUTY_FINDING_JSON_OBJECT` è l'ID risultato descritto precedentemente.

Creazione di una EventBridge regola per GuardDuty i risultati

Le seguenti procedure spiegano come utilizzare la EventBridge console Amazon e [AWS Command Line Interface \(AWS CLI\)](#) per creare una EventBridge regola per GuardDuty i risultati. La regola rileva EventBridge gli eventi che utilizzano lo schema e il pattern degli eventi per GuardDuty i risultati e invia tali eventi a una AWS Lambda funzione per l'elaborazione.

AWS Lambda è un servizio di elaborazione che è possibile utilizzare per eseguire codice senza fornire o gestire server. Impacchettate il codice e lo caricate AWS Lambda come funzione Lambda. AWS Lambda quindi esegue la funzione quando la funzione viene richiamata. Puoi richiamare una funzione manualmente, come risposta automatica agli eventi o in risposta a richieste provenienti da applicazioni o servizi. Per ulteriori informazioni su come creare e richiamare le funzioni Lambda, consulta [Guida per gli sviluppatori di AWS Lambda](#).

Scegliete il metodo preferito per creare una EventBridge regola che invii i GuardDuty risultati a un bersaglio.

Console

Segui questi passaggi per utilizzare la EventBridge console Amazon per creare una regola che invii automaticamente tutti gli eventi di GuardDuty ricerca a una funzione Lambda per l'elaborazione. La regola utilizza le impostazioni predefinite per le regole che vengono eseguite quando vengono ricevuti eventi specifici. Per dettagli sulle impostazioni delle regole o per scoprire come creare una regola che utilizza impostazioni personalizzate, consulta la sezione [Creazione di regole che reagiscono agli eventi](#) nella Amazon EventBridge User Guide.

Prima di creare questa regola, create la funzione Lambda che desiderate che la regola utilizzi come destinazione. Quando crei la regola, dovrai specificare questa funzione come sua destinazione. Il tuo obiettivo può anche essere l'argomento SNS che hai creato in precedenza. Per ulteriori informazioni, consulta [Configura un argomento e un endpoint di Amazon SNS \(Email, Slack e Amazon Chime\)](#).

Per creare una regola di evento utilizzando la console

1. Accedi a Console di gestione AWS e apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, in Autobus, scegli Regole.
3. Nella sezione Rules (Regole), scegli Create rule (Crea regola).
4. Nella pagina di dettaglio Definisci regola, procedi come segue:

- a. In Name (Nome), inserisci un nome per la regola.
 - b. (Facoltativo) In Descrizione, inserisci una breve descrizione della regola.
 - c. Per Event bus, assicuratevi che sia selezionato il valore predefinito e che l'opzione Abilita la regola sul bus eventi selezionato sia attivata.
 - d. Per Tipo di regola, scegli Regola con un modello di eventi.
 - e. Al termine, selezionare Next (Avanti).
5. Nella pagina Crea modello di eventi, procedi come segue:
- a. Per Origine dell'evento, scegli AWS eventi o eventi EventBridge partner.
 - b. (Facoltativo) Per un evento di esempio, esamina un esempio di evento di ricerca GuardDuty per scoprire cosa potrebbe contenere un evento. Per fare ciò, scegli AWS gli eventi. Quindi, per Eventi di esempio, scegli GuardDutyRicerca.
 - c. Opzione 1: utilizzo di pattern form, un modello che EventBridge fornisce

Nella sezione Event pattern, puoi fare quanto segue:

1. Per Metodo di creazione, seleziona Usa modulo modello.
2. In Event source (Origine eventi), selezionare Servizi AWS.
3. Per Servizio AWS, scegliere GuardDuty.
4. Per Tipo di evento, scegliete GuardDuty Ricerca.

Al termine, selezionare Next (Avanti).

- d. Opzione 2: utilizzo di un modello di eventi personalizzato in JSON

Nella sezione Event pattern, puoi fare quanto segue:

1. Per Metodo di creazione, seleziona Modello personalizzato (editor JSON).
2. Per Event pattern, incolla il seguente codice JSON personalizzato che creerà un avviso per risultati medi, alti e critici. Per ulteriori informazioni, consulta [Livelli di gravità dei risultati](#).

```
{
  "source": [
    "aws.guardduty"
  ],
  "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  
  ]  
}  
}
```

Al termine, selezionare Next (Avanti).

6. Opzione A - Selezione Servizio AWS - AWS Lambda come obiettivo

Nella pagina Seleziona obiettivi, procedi come segue:

- a. Per i tipi di destinazione, selezionare Servizio AWS.
- b. Per Select a target (Seleziona destinazione), scegli Lambda function (Funzione Lambda).
Quindi, per Funzione, scegliete la funzione Lambda a cui inviare gli eventi di ricerca.

- c. Per Configura versione/alias, inserisci le impostazioni della versione o dell'alias per la funzione Lambda di destinazione.
 - d. (Facoltativo) Per Impostazioni aggiuntive, immettete impostazioni personalizzate per specificare quali dati degli eventi desiderate inviare alla funzione Lambda. Puoi anche specificare come gestire gli eventi che non vengono consegnati correttamente alla funzione.
 - e. Al termine, selezionare Next (Avanti).
7. Opzione B - Selezione dell'argomento SNS come destinazione

Nella pagina Seleziona obiettivi, procedi come segue:

- a. Per i tipi di destinazione, selezionare Servizio AWS.
- b. Per Seleziona una destinazione, scegli Argomento SNS. Quindi, per Posizione di destinazione, seleziona l'opzione adatta in base alla posizione di destinazione. Per Argomento, scegli il nome dell'argomento SNS che hai creato.
- c. Espandere Additional settings (Impostazioni aggiuntive). Per Configura l'input target, scegli Input transformer.
- d. Seleziona Configura il trasformatore di input.
- e. Copia il codice seguente e incollalo nel campo Input Path nella sezione Target input transformer.

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

- f. Copia il codice seguente e incollalo nel campo Modello per formattare l'email.

```
"You have a severity <severity> GuardDuty finding type <Finding_Type> in the
<region> Region."
"Finding Description:"
"<Finding_description>. "
```

```
"For more details open the GuardDuty console at https://  
console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id  
%3D<Finding_ID>"
```

8. Nella pagina Configura tag, inserisci facoltativamente uno o più tag da assegnare alla regola. Quindi scegli Successivo.
9. Nella pagina Rivedi e crea, rivedi le impostazioni della regola e verifica che siano corrette.

Per modificare un'impostazione, scegli Modifica nella sezione che contiene l'impostazione, quindi inserisci l'impostazione corretta. Puoi anche utilizzare le schede di navigazione per andare alla pagina che contiene un'impostazione.

10. Al termine della verifica delle impostazioni, scegli Crea regola.

API

La procedura seguente mostra come utilizzare AWS CLI i comandi per creare una EventBridge regola e un obiettivo per GuardDuty. In particolare, la procedura mostra come creare una regola che EventBridge consenta di inviare eventi per tutti i risultati GuardDuty generati a una AWS Lambda funzione come destinazione della regola.

Note

In questo esempio, stiamo usando una funzione Lambda come obiettivo per la regola che si attiva. EventBridge Puoi anche configurare altre AWS risorse come obiettivi da attivare. EventBridge GuardDuty e EventBridge supportano i seguenti tipi di destinazione: istanze Amazon EC2, flussi Amazon Kinesis, attività Amazon ECS, macchine a stati AWS Step Functions , comandi e destinazioni integrate. run Per ulteriori informazioni, [PutTargets](#) consulta Amazon EventBridge API Reference.

Per creare una regola e un target

1. Per creare una regola che EventBridge consenta di inviare eventi per tutti i risultati GuardDuty generati, esegui il seguente comando EventBridge CLI.

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guardduty\"]}"
```

Puoi personalizzare ulteriormente la regola in modo che indichi di EventBridge inviare eventi solo per un sottoinsieme dei risultati generati GuardDuty. Questo sottoinsieme è basato sull'attributo o sugli attributi di risultato specificati nella regola. Ad esempio, utilizzate il seguente comando CLI per creare una regola che EventBridge consenta di inviare solo eventi per i GuardDuty risultati con la gravità di 5 o 8:

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":  
{\"severity\":[5,8]}}"
```

A tale scopo, è possibile utilizzare uno qualsiasi dei valori di proprietà disponibili in JSON per GuardDuty i risultati.

2. Per collegare una funzione Lambda come destinazione per la regola creata nel passaggio 1, esegui il seguente comando CLI CloudWatch .

```
aws events put-targets --rule your-target-name --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your_function
```

Assicurati di sostituire *your-target-name* nel comando precedente con la tua effettiva funzione Lambda per gli GuardDuty eventi.

3. Per aggiungere le autorizzazioni necessarie per richiamare la destinazione, esegui il comando CLI di Lambda seguente.

```
aws lambda add-permission --function-name your-target-name --statement-id 1 --  
action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Assicurati di sostituire *your_function* nel comando precedente con la tua effettiva funzione Lambda per gli GuardDuty eventi.

EventBridge regola per ambienti con GuardDuty più account

Quando si utilizza un account GuardDuty amministratore delegato, è possibile visualizzare gli eventi generati negli account dei membri e agire utilizzando altre applicazioni e servizi. EventBridge le regole nell'account amministratore verranno attivate in base ai risultati applicabili degli account membro. Se configuri le notifiche di ricerca tramite EventBridge il tuo account amministratore, riceverai notifiche sui risultati sia dal tuo account che dagli account dei membri. Ad esempio, è

possibile utilizzare per EventBridge inviare tipi specifici di risultati a una funzione Lambda che elabora e invia i dati al sistema di gestione degli incidenti e degli eventi di sicurezza (SIEM).

È possibile identificare l'account membro da cui ha avuto origine il GuardDuty risultato utilizzando il `accountId` campo dei dettagli JSON del risultato. Per creare una regola di evento personalizzata per account membri specifici, crea una nuova regola e utilizza il seguente modello in Event pattern. Sostituiscilo **123456789012** con quello `accountId` dell'account membro per il quale desideri attivare l'evento.

```
{
  "source": [
    "aws.guarddduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

Note

Questo esempio crea una regola che corrisponde a tutti i risultati dell'ID account specificato. È possibile includere più account IDs separandoli con virgole, seguendo la sintassi JSON.

Comprensione CloudWatch dei log e dei motivi per cui le risorse vengono ignorate durante la scansione Malware Protection for EC2

GuardDuty Malware Protection for EC2 pubblica gli eventi nel CloudWatch tuo gruppo di log Amazon/ aws/guarddduty/malware-scan-events. Puoi monitorare lo stato e il risultato della scansione delle risorse interessate per ciascuno degli eventi relativi alla scansione malware. Alcune risorse Amazon EC2 e volumi Amazon EBS potrebbero essere stati ignorati durante la scansione Malware Protection for EC2.

Controllo dei CloudWatch log in Malware Protection for EC2 GuardDuty

Esistono tre tipi di eventi di scansione supportati nel gruppo di log/aws/guardduty/malware CloudWatch -scan-events.

Nome dell'evento di scansione Malware Protection for EC2	Spiegazione
EC2_SCAN_STARTED	Creato quando un GuardDuty Malware Protection for EC2 avvia il processo di scansione antimalware, ad esempio quando si prepara a scattare un'istantanea di un volume EBS.
EC2_SCAN_COMPLETED	Creato al termine della scansione di GuardDuty Malware Protection for EC2 per almeno uno dei volumi EBS della risorsa interessata. Questo evento include anche lo snapshotId appartenente al volume EBS scansionato. Al termine della scansione, il risultato sarà CLEAN, THREATS_FOUND o NOT_SCANNED .
EC2_SCAN_SKIPPED	Creato quando la scansione di GuardDuty Malware Protection for EC2 ignora tutti i volumi EBS della risorsa interessata. Per identificare il motivo per cui vengono ignorati, seleziona l'evento corrispondente e visualizza i dettagli. Per ulteriori informazioni sui motivi per cui le risorse vengono ignorate, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware di seguito.

 Note

Se utilizzi un AWS Organizations, gli eventi di CloudWatch registro degli account dei membri in Organizations vengono pubblicati sia nell'account amministratore che nel gruppo di registro dell'account membro.

Scegli il metodo di accesso preferito per visualizzare e interrogare CloudWatch gli eventi.

Console

1. Accedi a Console di gestione AWS e apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, in Log, scegli Gruppi di log. Scegli il gruppo di log/aws/guardduty/malware-scan-events per visualizzare gli eventi di scansione per GuardDuty Malware Protection for EC2.

Per eseguire una query, scegli Log Insights.

Per informazioni sull'esecuzione di una query, consulta [Analyzing log data with CloudWatch Logs Insights](#) nella Amazon CloudWatch User Guide.

3. Scegli ID scansione per monitorare i dettagli della risorsa interessata e gli esiti relativi al malware. Ad esempio, puoi eseguire la seguente query per filtrare gli eventi di CloudWatch registro utilizzando. scanId Assicurati di utilizzare il tuo codice valido *scan-id*.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- Per lavorare con i gruppi di log, consulta la sezione [Ricerca AWS CLI nelle voci di log utilizzando l'Amazon CloudWatch User Guide](#).

Scegli il gruppo di log/aws/guardduty/malware-scan-events per visualizzare gli eventi di scansione per GuardDuty Malware Protection for EC2.

- Per visualizzare e filtrare gli eventi di log, consulta [GetLogEvents](#) e [FilterLogEvents](#), rispettivamente, in Amazon CloudWatch API Reference.

GuardDuty Protezione da malware per la conservazione dei log EC2

Il periodo di conservazione dei log predefinito per il gruppo di log `aws/guardduty/malware-scan-events` è di 90 giorni, dopodiché gli eventi di registro vengono eliminati automaticamente. Per modificare la politica di conservazione dei log per il tuo gruppo di CloudWatch log, consulta [Change log data retention in CloudWatch Logs](#) nella Amazon CloudWatch User Guide o [PutRetentionPolicy](#) nell'Amazon CloudWatch API Reference.

Motivi per cui una risorsa viene ignorata durante la scansione malware

Negli eventi relativi alla scansione malware, alcune risorse EC2 e alcuni volumi EBS potrebbero essere stati ignorati durante il processo di scansione. La tabella seguente elenca i motivi per cui GuardDuty Malware Protection for EC2 potrebbe non scansionare le risorse. Se applicabile, utilizza i passaggi proposti per risolvere questi problemi ed esegui la scansione di queste risorse la prossima volta che GuardDuty Malware Protection for EC2 avvia una scansione antimalware. Gli altri problemi vengono utilizzati per informarti sul corso degli eventi e non possono essere risolti.

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
RESOURCE_NOT_FOUND	La scansione antimalware <code>resourceArn</code> fornita per avviare la scansione antimalware su richiesta non è stata trovata nell'ambiente in uso. AWS	Convalida il <code>resourceArn</code> dell'istanza Amazon EC2 o del carico di lavoro di un container e riprova.	
ACCOUNT_INELIGIBLE	L'ID AWS dell'account da cui hai provato ad avviare una scansione antimalware su richiesta non è abilitato. GuardDuty	Verifica che GuardDuty sia abilitato per questo AWS account. Quando ne GuardDuty abiliti uno nuovo Regione AWS ,	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
		la sincronizzazione potrebbe richiedere fino a 20 minuti.	
UNSUPPORT ED_KEY_EN CRYPTION	GuardDuty Malware Protection for EC2 supporta volumi non crittografati e crittografati con chiave gestita dal cliente. Non supporta la scansione di volumi EBS crittografati utilizzando la Crittografia di Amazon EBS. Attualmente, esiste una differenza regionale per cui questo motivo di salto non è applicabile. Per ulteriori informazioni su questi aspetti Regioni AWS, vedere. Disponibilità di funzionalità specifiche per ogni regione	Sostituisci la chiave di crittografia con una chiave gestita dal cliente. Per ulteriori informazioni sui tipi di crittografia GuardDuty supportati, vedere Volumi Amazon EBS supportati per la scansione di malware.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
EXCLUDED_BY_SCAN_SETTINGS	L'istanza EC2 o il volume EBS sono stati esclusi durante la scansione malware. Esistono due motivazioni possibili: il tag è stato aggiunto all'elenco di inclusione, ma la risorsa non è associata a questo tag, il tag è stato aggiunto all'elenco di esclusione e la risorsa è associata a questo tag oppure il tag GuardDuty Excluded è impostato su true per questa risorsa.	Aggiorna le opzioni di scansione o i tag associati alla tua risorsa Amazon EC2. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente .	
UNSUPPORTED_VOLUME_SIZE	Il volume è superiore a 2048 GB.	Non utilizzabile.	
NO_VOLUME_ATTACHED	GuardDuty Malware Protection for EC2 ha rilevato l'istanza nel tuo account, ma nessun volume EBS è stato collegato a questa istanza per procedere con la scansione.	Non utilizzabile.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
UNABLE_TO_SCAN	Si tratta di un errore interno del servizio.	Non utilizzabile.	
SNAPSHOT_NOT_FOUND	Le istantanee create dai volumi EBS e condivise con l'account del servizio non sono state trovate e GuardDuty Malware Protection for EC2 non è riuscito a procedere con la scansione.	Verifica che CloudTrail le istantanee non siano state rimosse intenzionalmente.	
SNAPSHOT_QUOTA_REACHED	Hai raggiunto il volume massimo consentito per gli snapshot per ogni regione. Per questo motivo non è possibile né conservare né creare nuovi snapshot.	Puoi rimuovere gli snapshot meno recenti o richiederne un aumento della quota. Puoi visualizzare il limite predefinito per gli snapshot per ogni regione e scoprire come richiedere l'aumento della quota in Service Quotas nella Guida di riferimento generale di AWS .	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Più di 11 volumi EBS sono stati collegati a un'istanza EC2. GuardDuty Malware Protection for EC2 ha analizzato i primi 11 volumi EBS, ottenuti ordinandoli alfabeticamente. deviceName	Non utilizzabile.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
UNSUPPORT ED_PRODUC T_CODE_TYPE	GuardDuty può scansionare la maggior parte delle istanze con as. productCode marketplace Alcune istanze del marketplace potrebbero non essere idonee alla scansione. GuardDuty ignorerà tali istanze e registrerà il motivo come. UNSUPPORT ED_PRODUC T_CODE_TYPE Questo supporto varia a AWS GovCloud (US) seconda delle regioni della Cina. Per ulteriori informazioni, consulta Disponibilità di funzionalità specifiche per ogni regione. Per ulteriori informazioni, consulta Paid AMIs in the Amazon EC2 User Guide. Per informazioni su productCode , consulta ProductCo	Non utilizzabile.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
	de , nella Documentazione di riferimento delle API di Amazon EC2.		

Segnalazione di falsi positivi in Malware Protection for EC2

GuardDuty La protezione da malware per le EC2 scansioni può identificare un file innocuo nel carico di lavoro dell' EC2 istanza Amazon o del container come dannoso o dannoso. Per migliorare la tua esperienza con Malware Protection for EC2 e il GuardDuty servizio, puoi segnalare risultati falsi positivi se ritieni che un file identificato come dannoso o dannoso durante una scansione non contenga effettivamente malware.

Per segnalare un risultato di scansione EC2 antimalware di Amazon come falso positivo

Per avviare il processo, contatta Supporto. Utilizza i seguenti passaggi per fornire dettagli sulla risorsa scansionata:

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Scegli EC2 Malware Scans.
3. Scegli una scansione per visualizzare l'ID risultato.
4. Fornisci l'ID risultato. Devi fornire anche l'hash SHA-256 del file Ciò è necessario per garantire che GuardDuty Malware Protection for EC2 abbia ricevuto il file corretto.
5. Il Supporto team ti fornirà un URL predefinito di Amazon Simple Storage Service (Amazon S3) che potrai utilizzare per caricare il file potenzialmente dannoso e l'hash SHA-256. Per informazioni sui passaggi per caricare l'oggetto scansionato, consulta [Uploading objects with presigned URLs](#) nella Amazon S3 User Guide.
6. Dopo aver caricato il file, informa il team. Supporto

Supporto Fornirà un riconoscimento dopo aver ricevuto il file. I membri del team di GuardDuty assistenza analizzeranno la richiesta e prenderanno le misure appropriate per migliorare

l'esperienza dell'utente con Malware Protection for EC2 e il servizio. GuardDuty Il Supporto team continuerà a fornire aggiornamenti sullo stato del caso. GuardDuty conserva il tuo oggetto S3 per non più di 30 giorni.

Segnalazione del risultato della scansione degli oggetti S3 come falso positivo in Malware Protection for S3

Una scansione di Malware Protection for S3 può identificare un oggetto come potenzialmente dannoso o dannoso. Se ritieni che l'oggetto S3 indicato non contenga malware, segnala il risultato della scansione antimalware come falso positivo.

Puoi inviare una segnalazione di falsi positivi anche se utilizzi Malware Protection for S3 in modo indipendente. In questo caso, non GuardDuty è progettato per generare un risultato. Per informazioni sulla verifica dello stato della scansione e dello stato dei risultati, vedere [Monitoraggio delle scansioni degli oggetti S3](#).

Per segnalare un oggetto S3 (malware), il risultato della scansione è falso positivo.

Per avviare il processo, contatta. Supporto Utilizza i seguenti passaggi per fornire dettagli sull'oggetto S3 scansionato:

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. A seconda del caso d'uso, scegli i passaggi appropriati:

Using Malware Protection for S3 with GuardDuty

1. Nel riquadro di navigazione, seleziona Esiti.
2. Nella pagina Risultati, seleziona il risultato falso positivo per visualizzarne i dettagli.
3. Controllando i dettagli del risultato, fornisci l'ID del risultato, la regione, il nome del bucket S3 protetto e la chiave dell'oggetto scansionato.

Dai dettagli del percorso dell'elemento, fornisci l'hash dell'oggetto. Ciò è necessario per assicurarsi di aver GuardDuty ricevuto il file corretto.

Using Malware Protection for S3 independently

Fornisci il nome del bucket S3 protetto, il nome dell'oggetto scansionato e il. Regione AWS

3. Il Supporto team ti fornirà un URL predefinito di Amazon Simple Storage Service (Amazon S3) che potrai utilizzare per caricare il file e l'hash potenzialmente dannosi. Per informazioni sui passaggi per caricare l'oggetto scansionato, consulta [Uploading objects with presigned URLs](#) nella Amazon S3 User Guide.
4. Dopo aver caricato l'oggetto S3, informa il team. Supporto

Supporto Fornirà una conferma di ricezione dell'oggetto. I membri del team di GuardDuty assistenza analizzeranno la richiesta e prenderanno le misure appropriate per migliorare l'esperienza dell'utente con Malware Protection for S3 e il servizio. GuardDuty Il Supporto team continuerà a fornire aggiornamenti sullo stato del caso. GuardDuty conserva il tuo oggetto S3 per non più di 30 giorni.

Segnalazione di falsi positivi in Malware Protection for Backup

Per migliorare la tua esperienza con GuardDuty Malware Protection for Backup, puoi segnalare potenziali falsi positivi e falsi negativi.

Per segnalare un potenziale falso positivo o falso negativo identificato in Malware Protection for Backup

Per avviare il processo, contattare Supporto. Utilizza i seguenti passaggi per fornire dettagli sulla risorsa scansionata:

1. Accedi a Console di gestione AWS e apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Scegli Scansioni malware.
3. Scegli una scansione per visualizzare l'ID risultato.
4. Fornisci l'ID risultato. Devi fornire anche l'hash SHA-256 del file Ciò è necessario per assicurarsi di GuardDuty aver ricevuto il file corretto. Fornisci anche la regione da cui invierai il campione.
5. Il Supporto team ti fornirà un URL predefinito di Amazon Simple Storage Service (Amazon S3) che utilizzerai per caricare il file potenzialmente dannoso e l'hash SHA-256. Per informazioni sui passaggi per caricare la risorsa scansionata, consulta [Uploading objects with presigned URLs](#) nella Amazon S3 User Guide.
6. Dopo aver caricato il file, informa il team. Supporto

Supporto Fornirà un riconoscimento dopo aver ricevuto il file. I membri del team di GuardDuty assistenza analizzeranno la tua richiesta e adotteranno le misure appropriate per migliorare

la tua esperienza con Malware Protection for. EC2 Il Supporto team continuerà a fornire aggiornamenti sullo stato del caso. GuardDuty conserva il tuo oggetto S3 per non più di 30 giorni.

Correzione dei problemi di GuardDuty sicurezza rilevati

Amazon GuardDuty genera [risultati](#) che indicano potenziali problemi di sicurezza associati al rilevamento delle minacce GuardDuty di base e ai piani di protezione dedicati. Le sezioni seguenti descrivono le operazioni di correzione consigliate per questi scenari. Se esistono scenari di riparazione alternativi, questi verranno descritti nelle descrizioni di ogni tipo di risultato. Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla [tabella relativa ai tipi di esiti attivi](#).

Indice

- [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#)
- [Riparazione di un bucket S3 potenzialmente compromesso](#)
- [Riparazione di un oggetto S3 potenzialmente dannoso](#)
- [Correzione di uno snapshot EBS potenzialmente compromesso](#)
- [Correzione di un AMI EC2 potenzialmente compromesso](#)
- [Riparazione di un punto di ripristino EC2 potenzialmente compromesso](#)
- [Riparazione di un punto di ripristino S3 potenzialmente compromesso](#)
- [Riparazione di un cluster ECS potenzialmente compromesso](#)
- [Riparazione delle credenziali potenzialmente compromesse AWS](#)
- [Riparazione di un contenitore autonomo potenzialmente compromesso](#)
- [Correzione dei risultati della protezione EKS](#)
- [Riparazione degli esiti del monitoraggio del runtime](#)
- [Ripristino di un database potenzialmente compromesso](#)
- [Correzione di una funzione Lambda potenzialmente compromessa](#)

Correzione di un'istanza Amazon EC2 potenzialmente compromessa

Quando vengono GuardDuty generati [tipi di ricerca che indicano risorse Amazon EC2 potenzialmente compromesse](#), la risorsa sarà l'istanza. I potenziali tipi di ricerca potrebbero essere [Tipi di esiti EC2GuardDuty](#) [Tipi di risultati del monitoraggio del runtime](#), o. [Protezione da malware per tipi di ricerca EC2](#) Se il comportamento che ha causato il risultato era previsto nel tuo ambiente, valuta la possibilità di utilizzarlo [Regole di eliminazione](#).

Esegui i seguenti passaggi per correggere l'istanza Amazon EC2 potenzialmente compromessa:

1. Identifica l'istanza Amazon EC2 potenzialmente compromessa

Ricerca malware nell'istanza potenzialmente compromessa e rimuovi quello rilevato. Puoi utilizzare la [Scansione antimalware su richiesta GuardDuty](#) per identificare un eventuale malware nell'istanza EC2 potenzialmente compromessa o verificare [Marketplace AWS](#) per capire se esistono prodotti di partner utili per identificare e rimuovere il malware.

2. Isolare l'istanza Amazon EC2 potenzialmente compromessa

Se possibile, utilizza i seguenti passaggi per isolare l'istanza potenzialmente compromessa:

1. Crea un gruppo di sicurezza Isolation dedicato. Un gruppo di sicurezza di isolamento deve avere accesso in entrata e in uscita solo da indirizzi IP specifici. Assicurati che non esista alcuna regola in entrata o in uscita che consenta il traffico di. 0.0.0.0/0 (0-65535)
2. Associate il gruppo di sicurezza Isolation a questa istanza.
3. Rimuovi tutte le associazioni dei gruppi di sicurezza diverse dal gruppo di sicurezza Isolation appena creato dall'istanza potenzialmente compromessa.

Note

Le connessioni tracciate esistenti non verranno interrotte a seguito della modifica dei gruppi di sicurezza: solo il traffico futuro verrà effettivamente bloccato dal nuovo gruppo di sicurezza.

Per informazioni su come bloccare ulteriore traffico proveniente da connessioni sospette esistenti, consulta Implementare in [NACLs base IoCs alla rete per prevenire ulteriore traffico nell'Incident Response Playbook](#).

3. Identifica l'origine dell'attività sospetta

Se viene rilevato un malware, in base al tipo di esito nel tuo account, identifica e interrompi l'attività potenzialmente non autorizzata sull'istanza EC2. Ciò potrebbe richiedere operazioni come la chiusura di tutte le porte aperte, la modifica delle policy di accesso e l'aggiornamento delle applicazioni per correggere le vulnerabilità.

Se non sei in grado di identificare e interrompere attività non autorizzate sulla tua istanza EC2 potenzialmente compromessa, ti consigliamo di terminare l'istanza EC2 compromessa e sostituirla

con una nuova istanza, se necessario. Le risorse supplementari seguenti ti consentono di proteggere ulteriormente le istanze EC2:

- Sezioni sulla sicurezza e sulle reti in [Best practice per Amazon EC2](#)
- [Gruppi di sicurezza Amazon EC2 per istanze Linux](#).
- [Sicurezza in Amazon EC2](#)
- [Suggerimenti per la protezione dell'istanza EC2 \(Linux\)](#)
- [AWS migliori pratiche di sicurezza](#)
- [AWS Guida tecnica sulla risposta agli incidenti di sicurezza](#).

4. Sfoglia AWS re:Post

Naviga [AWS re:Post](#) per ulteriore assistenza.

5. Invia una richiesta di supporto tecnico

Se sei abbonato a un pacchetto Premium Support, puoi inviare una richiesta di [supporto tecnico](#).

Riparazione di un bucket S3 potenzialmente compromesso

Quando viene GuardDuty generato [GuardDuty S3 Tipi di risultati di protezione](#), indica che i bucket Amazon S3 sono stati compromessi. Se il comportamento che ha causato il risultato era previsto nel tuo ambiente, valuta la possibilità di crearlo. [Regole di eliminazione](#) Se questo comportamento non era previsto, segui questi passaggi consigliati per correggere un bucket Amazon S3 potenzialmente compromesso nel tuo ambiente: AWS

1. Identifica la risorsa S3 potenzialmente compromessa.

Un GuardDuty risultato per S3 elencherà il bucket S3 associato, il relativo Amazon Resource Name (ARN) e il suo proprietario nei dettagli del risultato.

2. Identifica l'origine dell'attività sospetta e la chiamata API utilizzata.

La chiamata API utilizzata verrà elencata come API nei dettagli del risultato. L'origine sarà un principale IAM (un ruolo, un utente o un account IAM) e i dettagli identificativi verranno elencati nell'esito. A seconda del tipo di origine, saranno disponibili informazioni sull'indirizzo IP remoto o sul dominio di origine che servono per valutare se l'origine era autorizzata o meno. Se il risultato riguardava credenziali di un'istanza Amazon EC2, verranno inclusi anche i dettagli per quella risorsa.

3. Determina se l'origine della chiamata era autorizzata ad accedere alla risorsa identificata.

Ad esempio, considera i quesiti seguenti:

- Se è stato coinvolto un utente IAM, è possibile che le sue credenziali siano state potenzialmente compromesse? Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).
- Se un'API è stata richiamata da un principale che non aveva mai invocato questo tipo di API in precedenza, l'origine in questione necessita delle autorizzazioni di accesso per questa operazione? Le autorizzazioni del bucket possono essere ulteriormente limitate?
- Se l'accesso è stato visualizzato dal nome utente ANONYMOUS_PRINCIPAL con tipo di utente di AWSAccount, significa che il bucket è pubblico e vi è stato effettuato l'accesso. Questo bucket dovrebbe essere pubblico? In caso negativo, consulta i consigli di sicurezza riportati di seguito per trovare soluzioni alternative alla condivisione delle risorse S3.
- Se l'accesso è avvenuto tramite una chiamata PreflightRequest riuscita visualizzata dal nome utente ANONYMOUS_PRINCIPAL con tipo di utente AWSAccount, significa che il bucket ha un set di policy di condivisione delle risorse multiorigine (CORS). Questo bucket dovrebbe avere una policy CORS? In caso negativo, assicurati che il bucket non sia stato involontariamente reso pubblico e consulta i consigli di sicurezza riportati di seguito per trovare soluzioni alternative alla condivisione delle risorse S3. Per ulteriori informazioni su CORS, consulta [Utilizzo delle funzionalità Cross-Origin Resource Sharing \(CORS\)](#) nella Guida per l'utente di S3.

4. Determina se il bucket S3 contiene dati sensibili.

Usa [Amazon Macie](#) per determinare se il bucket S3 contiene dati sensibili, come informazioni di identificazione personale (PII), dati finanziari o credenziali. Se il rilevamento automatico dei dati sensibili è abilitato per il tuo account Macie, esamina i dettagli del bucket S3 per comprendere meglio il contenuto del bucket S3. Se questa funzionalità è disabilitata per il tuo account Macie, ti consigliamo di attivarla per accelerare la valutazione. In alternativa, puoi creare ed eseguire un processo di rilevamento dei dati sensibili per ispezionare gli oggetti del bucket S3 alla ricerca di dati sensibili. Per ulteriori informazioni, consulta [Rilevamento dei dati sensibili con Macie](#).

Se l'accesso era autorizzato, puoi ignorare l'esito. La <https://console.aws.amazon.com/guardduty/console> consente di impostare regole per eliminare completamente i risultati individuali in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

Se ritieni che i tuoi dati S3 siano stati esposti o consultati da soggetti non autorizzati, consulta i seguenti consigli sulla sicurezza di S3 per rafforzare le autorizzazioni e limitare l'accesso. Le soluzioni di correzione appropriate dipenderanno dalle esigenze dell'ambiente specifico.

Consigli basati su esigenze specifiche di accesso ai bucket S3

L'elenco seguente fornisce consigli basati su esigenze specifiche di accesso ai bucket Amazon S3:

- Per limitare l'accesso pubblico all'uso dei dati S3 in modo centralizzato, S3 blocca l'accesso pubblico. Le impostazioni di blocco dell'accesso pubblico possono essere abilitate per punti di accesso, bucket e AWS account tramite quattro diverse impostazioni per controllare la granularità dell'accesso. Per ulteriori informazioni, consulta [Blocca le impostazioni di accesso pubblico](#) nella Guida per l'utente di Amazon S3.
- AWS Le policy di accesso possono essere utilizzate per controllare in che modo gli utenti IAM possono accedere alle tue risorse o come accedere ai tuoi bucket. Per ulteriori informazioni, consulta [Using bucket policies and user policies](#) nella Amazon S3 User Guide.

Inoltre, puoi utilizzare gli endpoint del cloud privato virtuale (VPC) con policy del bucket S3 per limitare l'accesso a endpoint VPC specifici. Per ulteriori informazioni, consulta [Controllare l'accesso dagli endpoint VPC con le policy dei bucket nella Guida per l'utente di Amazon S3](#).

- Per consentire temporaneamente l'accesso ai tuoi oggetti S3 a entità attendibili esterne al tuo account, puoi creare un URL prefirmato tramite S3. Questo accesso viene creato utilizzando le credenziali dell'account e, a seconda delle credenziali utilizzate, può durare da 6 ore a 7 giorni. Per ulteriori informazioni, consulta [Using presigned URLs to download and upload objects](#) nella Amazon S3 User Guide.
- Per i casi d'uso che richiedono la condivisione di oggetti S3 tra diverse origini, puoi utilizzare i punti di accesso S3 per creare set di autorizzazioni che limitano l'accesso solo a quelli che si trovano all'interno della tua rete privata. Per ulteriori informazioni, consulta [Gestire l'accesso a set di dati condivisi con punti di accesso](#) nella Amazon S3 User Guide.
- Per concedere l'accesso sicuro alle tue risorse S3 ad altri AWS account puoi utilizzare una lista di controllo degli accessi (ACL). Per ulteriori informazioni, consulta la [panoramica della lista di controllo degli accessi \(ACL\)](#) nella Guida per l'utente di Amazon S3.

Per ulteriori informazioni sulle opzioni di sicurezza di S3, consulta le [best practice di sicurezza per Amazon S3 nella Amazon S3 User Guide](#).

Riparazione di un oggetto S3 potenzialmente dannoso

Quando viene GuardDuty generato [Protezione da malware per tipo di ricerca S3](#), indica che un oggetto appena caricato nel bucket Amazon S3 contiene malware. Il tipo di risorsa è un S3Object.

Utilizza i seguenti passaggi consigliati per correggere potenzialmente il risultato generato:

1. Identifica l'oggetto S3 potenzialmente dannoso controllando l'S3 ObjectDetails associato al risultato.
2. Isola l'oggetto S3 interessato. Se avevi abilitato il tagging al momento dell'attivazione di Malware Protection for S3 per il bucket Amazon S3 associato GuardDuty, devi aver assegnato un tag Malicious a questo oggetto. Utilizza il controllo degli accessi basato su tag (TBAC) per limitare l'accesso a questo oggetto S3. Per ulteriori informazioni, consulta [Utilizzo del controllo degli accessi basato su tag \(TBAC\)](#).

In alternativa, se non hai più bisogno di questo oggetto, puoi anche scegliere di eliminarlo o spostarlo in un bucket S3 isolato. Per informazioni sulle considerazioni relative all'eliminazione di un oggetto S3, consulta [Eliminazione di oggetti](#) nella Amazon S3 User Guide.

Correzione di uno snapshot EBS potenzialmente compromesso

Quando genera GuardDuty un'esecuzione:EC2/MaliciousFile Tipo di ricerca di snapshot, indica che è stato rilevato malware in uno snapshot di Amazon EBS. Esegui i seguenti passaggi per correggere lo snapshot potenzialmente compromesso:

1. Identifica l'istantanea potenzialmente compromessa
 1. Identifica l'istantanea potenzialmente compromessa. Un GuardDuty risultato per uno snapshot EBS elencherà l'ID dello snapshot interessato, il relativo Amazon Resource Name (ARN) e i dettagli della scansione del malware associata nei dettagli del risultato.
 2. Controlla i dettagli del punto di ripristino utilizzando il seguente comando:

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789 --recovery-point-arn "arn:aws:ec2:us-east-1::snapshot/snap-abcdef01234567890"
```

2. Limita l'accesso all'istantanea compromessa

Rivedi e modifica le politiche di accesso al backup vault per limitare l'accesso ai punti di ripristino e sospendere qualsiasi processo di ripristino automatico che potrebbe utilizzare questa istantanea.

1. Rivedi le attuali autorizzazioni di condivisione:

```
aws ec2 describe-snapshot-attribute --snapshot-id snap-abcdef01234567890 --  
attribute createVolumePermission
```

2. Rimuovi l'accesso specifico all'account:

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-abcdef01234567890 --  
attribute createVolumePermission --operation-type remove --user-ids 111122223333
```

3. [Per ulteriori opzioni CLI, consulta la documentazione CLImodify-snapshot-attribute](#).

3. Intraprendi azioni correttive

- Prima di procedere con l'eliminazione, assicurati di aver identificato tutte le dipendenze e di disporre di backup adeguati, se necessario.

Correzione di un AMI EC2 potenzialmente compromesso

Quando GuardDuty genera un'esecuzione:EC2/! MaliciousFile Tipo di rilevamento AMI, indica che è stato rilevato del malware in un'Amazon Machine Image (AMI). Esegui i seguenti passaggi per correggere l'AMI potenzialmente compromessa:

1. Identifica l'AMI potenzialmente compromessa

1. Un GuardDuty risultato per AMIs elencherà l'ID AMI interessato, il relativo Amazon Resource Name (ARN) e i dettagli della scansione del malware associata nei dettagli del risultato.
2. Rivedi l'immagine sorgente AMI:

```
aws ec2 describe-images --image-ids ami-021345abcdef6789
```

2. Limita l'accesso alle risorse compromesse

1. Rivedi e modifica le politiche di accesso al backup vault per limitare l'accesso ai punti di ripristino e sospendere qualsiasi processo di ripristino automatico che potrebbe utilizzare questo punto di ripristino.

2. Rimuovi le autorizzazioni dalle autorizzazioni AML di origine

Prima visualizza le autorizzazioni esistenti:

```
aws ec2 describe-image-attribute --image-id ami-abcdef01234567890 --attribute launchPermission
```

Quindi rimuovi le autorizzazioni individuali:

```
aws ec2 modify-image-attribute --image-id ami-abcdef01234567890 --launch-permission '{"Remove":[{"UserId":"111122223333"}]}'
```

Per ulteriori opzioni CLI, consulta [Condivisione di un'AMI con account specifici - Amazon Elastic Compute Cloud](#)

3. Se l'origine è un'istanza EC2, consulta: [Riparazione di un'istanza Amazon EC2 potenzialmente compromessa](#).

3. Intraprendi azioni correttive

- Prima di procedere con l'eliminazione, assicurati di aver identificato tutte le dipendenze e di disporre di backup adeguati, se necessario.

Riparazione di un punto di ripristino EC2 potenzialmente compromesso

Quando GuardDuty genera un'esecuzione:EC2/MaliciousFile RecoveryPoint individuando il tipo, indica che è stato rilevato del malware in una risorsa di EC2 Recovery Point Backup. Esegui i seguenti passaggi per correggere il punto di ripristino potenzialmente compromesso:

1. Identifica il punto di ripristino EC2 potenzialmente compromesso

1. Una GuardDuty scoperta per EC2 Recovery Point elencherà il suo Amazon Resource Name (ARN) e i dettagli della scansione del malware associata nei dettagli del risultato:

```
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-EXAMPLE11111"
```

2. Consulta i dettagli di ripristino per cercare l'immagine sorgente:

```
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-EXAMPLE11111"
```

2. Limita l'accesso alle risorse compromesse

- Rivedi e modifica le politiche di accesso al backup vault per limitare l'accesso ai punti di ripristino e sospendere qualsiasi processo di ripristino automatico che potrebbe utilizzare questo punto di ripristino. Se il tuo ambiente utilizza l'etichettatura delle risorse, contrassegna il punto di ripristino in modo appropriato per indicare che è oggetto di indagine e valuta la possibilità di sospendere i backup pianificati, se necessario.

Esempio:

```
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. Intraprendi azioni correttive

- Prima di procedere con l'eliminazione, assicurati di aver identificato tutte le dipendenze e di disporre di backup adeguati, se necessario.

Riparazione di un punto di ripristino S3 potenzialmente compromesso

Quando GuardDuty genera un Execution:S3/MaliciousFile RecoveryPoint individuando il tipo, indica che è stato rilevato del malware in una risorsa di S3 Recovery Point Backup. Esegui i seguenti passaggi per correggere il punto di ripristino potenzialmente compromesso:

1. Identifica il punto di ripristino S3 potenzialmente compromesso

1. Un GuardDuty risultato per i punti di ripristino S3 elencherà l'ARN del punto di ripristino interessato, il nome del backup vault e i dettagli della scansione del malware associata nei dettagli del risultato.
2. Rivedi i dettagli del punto di ripristino:

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789  
--recovery-point-arn arn:aws:backup:us-east-1:123456789012:recovery-  
point:abcdef01234567890
```

2. Limita l'accesso alle risorse compromesse

- Rivedi e modifica le politiche di accesso al backup vault per limitare l'accesso ai punti di ripristino e sospendere qualsiasi processo di ripristino automatico che potrebbe utilizzare questo punto di ripristino. Se il tuo ambiente utilizza l'etichettatura delle risorse, contrassegna il punto di ripristino in modo appropriato per indicare che è oggetto di indagine e valuta la possibilità di sospendere i backup pianificati, se necessario.

Esempio:

```
aws backup tag-resource --resource-arn arn:aws:backup:us-  
east-1:111122223333:recovery-point:abcdef01234567890 --  
tags Investigation=Malware,DoNotDelete=True
```

Per ulteriori dettagli, vedere: riferimento ai comandi [CLI tag-resource](#)

3. Intraprendi azioni correttive

- Prima di procedere con l'eliminazione, assicurati di aver identificato tutte le dipendenze e di disporre di backup adeguati, se necessario.

Riparazione di un cluster ECS potenzialmente compromesso

Un rilevamento di un cluster ECS potenzialmente compromesso indica che sono state rilevate attività sospette o dannose all'interno del tuo ambiente Amazon ECS. Ciò potrebbe includere l'accesso non autorizzato, l'esecuzione di malware o altri comportamenti dannosi che mettono a rischio i carichi di lavoro dei container.

Segui questi passaggi per correggere un cluster Amazon ECS potenzialmente compromesso:

1. Identifica il cluster ECS potenzialmente compromesso e la minaccia rilevata (risultati)

I dettagli del cluster ECS interessato sono elencati nel pannello dei dettagli dei GuardDuty risultati.

2. Valuta l'origine della minaccia/del malware

Verifica la presenza di malware nelle immagini dei container. Se viene rilevato del malware, esamina l'immagine del contenitore utilizzata. Consente [ListTasks](#) di identificare tutte le altre attività in esecuzione che utilizzano la stessa immagine potenzialmente compromessa.

3. Isolare le attività interessate

Blocca la minaccia bloccando tutto il traffico di rete (in entrata e in uscita) diretto alle attività interessate. Questo isolamento della rete aiuta a prevenire eventuali attacchi continui interrompendo tutte le connessioni all'attività compromessa.

Nota: se si determina che questo risultato è stato determinato da expected/legitimate un'attività nel proprio ambiente, è possibile impostare una regola di soppressione per evitare che vengano visualizzati risultati simili. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

Riparazione delle credenziali potenzialmente compromesse AWS

Quando viene GuardDuty generata [Tipi di esiti IAM](#), indica che le AWS credenziali sono state compromesse. Il tipo di risorsa potenzialmente compromesso è. AccessKey

Per correggere le credenziali potenzialmente compromesse nel tuo AWS ambiente, procedi come segue:

1. Identifica l'entità IAM potenzialmente compromessa e la chiamata API utilizzata.

La chiamata API utilizzata verrà elencata come API nei dettagli del risultato. L'entità IAM (un ruolo o un utente IAM) e le relative informazioni identificative verranno elencate nella sezione Risorse dei dettagli del risultato. Il tipo di entità IAM coinvolta può essere determinato dal campo Tipo utente, il nome dell'entità IAM sarà nel campo Nome utente . Il tipo di entità IAM coinvolta nel risultato può anche essere determinato dall'ID chiave di accesso utilizzato.

Per le chiavi che iniziano con AKIA:

Questo tipo di chiave è una credenziale gestita dal cliente a lungo termine associata a un utente IAM o Utente root dell'account AWS. Per informazioni sulla gestione delle chiavi di accesso per gli utenti IAM, consulta [Gestione delle chiavi di accesso per gli utenti IAM](#).

Per le chiavi che iniziano con ASIA:

Questo tipo di chiave è una credenziale temporanea a breve termine generata da AWS Security Token Service. Queste chiavi esistono solo per un breve periodo e non possono

essere visualizzate o gestite nella console di AWS gestione. I ruoli IAM utilizzeranno sempre AWS STS le credenziali, ma possono anche essere generate per gli utenti IAM, per ulteriori informazioni, AWS STS consulta [IAM: Temporary security credentials](#).

Se è stato utilizzato un ruolo, il campo Nome utente indicherà il nome del ruolo utilizzato. Puoi determinare in che modo è stata richiesta la chiave AWS CloudTrail esaminando l'elemento della voce di CloudTrail registro, per maggiori informazioni consulta [IAM e AWS STS](#) information in. CloudTrail

2. Esaminare le autorizzazioni per l'entità IAM.

Apri la console IAM. A seconda del tipo di entità utilizzata, scegli la scheda Utenti o Ruoli e individua l'entità interessata digitando il nome identificato nel campo di ricerca. Utilizzare le schede Autorizzazione e Access Advisor per esaminare le autorizzazioni effettive per tale entità.

3. Stabilire se le credenziali dell'entità IAM sono state utilizzate legittimamente.

Contattare l'utente delle credenziali per stabilire se l'attività era intenzionale.

Ad esempio, determina se l'utente ha:

- Ha richiamato l'operazione API elencata nel risultato GuardDuty
- Chiamato l'operazione API all'ora indicata nel risultato GuardDuty
- Chiamato l'operazione API dall'indirizzo IP indicato nel risultato GuardDuty

Se questa attività è un uso legittimo delle AWS credenziali, puoi ignorare il GuardDuty risultato. La <https://console.aws.amazon.com/guardduty/console> consente di impostare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

Se non riesci a confermare se questa attività è un uso legittimo, potrebbe essere il risultato di una compromissione di una particolare chiave di accesso: le credenziali di accesso dell'utente IAM o forse l'intera. Account AWS Se sospetti che le tue credenziali siano state compromesse, consulta le informazioni in Il [mio caso Account AWS potrebbe essere compromesso](#) per risolvere il problema.

Riparazione di un contenitore autonomo potenzialmente compromesso

Quando vengono GuardDuty generati [tipi di ricerca che indicano un contenitore potenzialmente compromesso](#), il tipo di risorsa sarà Contenitore. Se il comportamento che ha causato il risultato era previsto nel tuo ambiente, prendi in considerazione l'utilizzo [Regole di eliminazione](#).

Per correggere le credenziali potenzialmente compromesse nell' AWS ambiente, effettuate le seguenti operazioni:

1. Isolare il contenitore potenzialmente compromesso

I seguenti passaggi ti aiuteranno a identificare il carico di lavoro dei container potenzialmente dannoso:

- Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
- Nella pagina Risultati, scegli il risultato corrispondente per visualizzare il pannello dei risultati.
- Nel pannello degli esiti, nella sezione Risorsa interessata, puoi visualizzare l'ID e il nome del container.

Isola questo container dagli altri carichi di lavoro del container.

2. Metti in pausa il container

Sospendi tutti i processi nel container.

Per informazioni sul congelamento del contenitore, consulta Mettere in [pausa un](#) contenitore.

Fermate il contenitore.

Se la fase precedente ha esito negativo e il container non si ferma, arrestane il funzionamento. Se hai abilitato la [Conservazione delle istantanee](#) funzione, GuardDuty conserverà le istantanee dei tuoi volumi EBS che contengono malware.

Per informazioni sull'arresto del contenitore, consulta [Stop](#) a container.

3. Valuta la presenza di malware

Valuta se nell'immagine del container è presente un malware.

Se l'accesso era autorizzato, puoi ignorare l'esito. La <https://console.aws.amazon.com/guardduty/console> consente di impostare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. La GuardDuty console consente di impostare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta [Regole di soppressione in GuardDuty](#).

Correzione dei risultati della protezione EKS

Amazon GuardDuty genera [risultati](#) che indicano potenziali problemi di sicurezza di Kubernetes quando EKS Protection è abilitato per il tuo account. Per ulteriori informazioni, consulta [Protezione EKS](#). Le sezioni seguenti descrivono le operazioni di correzione consigliate per questi scenari. Le operazioni correttive sono descritte nella voce relativa al tipo di esito specifico. Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla [tabella relativa ai tipi di esiti attivi](#).

Se uno qualsiasi dei tipi di risultati di EKS Protection è stato generato in modo prevedibile, puoi prendere in considerazione l'aggiunta [Regole di soppressione in GuardDuty](#) per prevenire avvisi futuri.

Diversi tipi di attacchi e problemi di configurazione possono attivare i risultati di GuardDuty EKS Protection. Questa guida aiuta a identificare le cause principali delle GuardDuty rilevazioni relative al cluster e delinea le linee guida appropriate per la correzione. Le seguenti sono le cause principali che hanno portato ai risultati di GuardDuty Kubernetes:

- [Potenziali problemi di configurazione](#)
- [Riparare gli utenti Kubernetes potenzialmente compromessi](#)
- [Riparazione dei pod Kubernetes potenzialmente compromessi](#)
- [Riparazione dei nodi Kubernetes potenzialmente compromessi](#)
- [Riparazione delle immagini dei container potenzialmente compromesse](#)

Note

Prima della versione 1.14 di Kubernetes, il `system:unauthenticated` gruppo era associato a e per impostazione predefinita. `system:discovery` `system:basic-user` ClusterRoles. Ciò potrebbe consentire l'accesso non intenzionale a utenti anonimi. Gli aggiornamenti del cluster non revocano le autorizzazioni, quindi potrebbero essere ancora valide anche se hai aggiornato il cluster alla versione 1.14 o successiva. Ti consigliamo di disassociare queste autorizzazioni dal gruppo `system:unauthenticated`.

Per ulteriori informazioni sulla rimozione di queste autorizzazioni, consulta [Proteggi i cluster Amazon EKS con le migliori pratiche](#) nella Guida per l'utente di Amazon EKS.

Potenziali problemi di configurazione

Se un esito indica un problema di configurazione, consulta la sezione sulla correzione di tale esito per indicazioni su come risolvere il problema. Per ulteriori informazioni, consulta i seguenti tipi di esiti che indicano problemi di configurazione:

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- Qualsiasi scoperta che finisce con `SuccessfulAnonymousAccess`

Riparare gli utenti Kubernetes potenzialmente compromessi

Un GuardDuty risultato può indicare un utente Kubernetes compromesso quando un utente identificato nel risultato ha eseguito un'azione API inaspettata. Puoi identificare l'utente nella sezione Dettagli utente Kubernetes dei dettagli di un esito nella console o nei `resource.kubernetesDetails.kubernetesUserDetails` del file JSON degli esiti. Questi dettagli utente includono `user name`, `uid` e i gruppi Kubernetes a cui appartiene l'utente.

Se l'utente accedeva al carico di lavoro utilizzando un'entità IAM, puoi utilizzare la sezione `Access Key details` per identificare i dettagli di un ruolo o di un utente IAM. Consulta i seguenti tipi di utente e le linee guida per la correzione.

Note

Puoi utilizzare Amazon Detective per esaminare ulteriormente il ruolo o l'utente IAM identificato nell'esito. Mentre visualizzi i dettagli del ritrovamento GuardDuty sulla console, scegli **Investiga in Detective**. Quindi seleziona AWS l'utente o il ruolo dagli elementi elencati per esaminarlo in Detective.

Amministratore Kubernetes integrato: l'utente predefinito assegnato da Amazon EKS all'identità IAM che ha creato il cluster. Questo tipo di utente è identificato dal nome utente `kubernetes-admin`.

Per revocare l'accesso a un amministratore Kubernetes integrato:

- Identifica il `userType` nella sezione `Access Key details`.
 - Se il `userType` è un Ruolo e il ruolo appartiene a un ruolo dell'istanza EC2:
 - Identifica l'istanza e segui le istruzioni riportate in [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).
 - Se il `userType` è un Utente o un Ruolo assunto da un utente:
 1. [Ruota la chiave di accesso](#) dell'utente.
 2. Ruota tutti i segreti a cui l'utente ha avuto accesso.
 3. Consulta le informazioni in [Il mio Account AWS potrebbe essere compromessa](#) per ulteriori dettagli.

Utente autenticato OIDC: un utente a cui è stato concesso l'accesso tramite un provider OIDC. In genere un utente OIDC ha un indirizzo e-mail come nome utente. Puoi verificare se il cluster utilizza OIDC con il comando seguente: `aws eks list-identity-provider-configs --cluster-name your-cluster-name`

Per revocare l'accesso a un utente autenticato OIDC:

1. Ruota le credenziali dell'utente nel provider OIDC.
2. Ruota tutti i segreti a cui l'utente ha avuto accesso.

AWS-Auth ConfigMap defined user: un utente IAM a cui è stato concesso l'accesso tramite un `-auth`. AWS ConfigMap Per ulteriori informazioni, consulta [la sezione Gestione degli utenti o dei ruoli IAM per il tuo cluster](#) nella Amazon EKS User Guide. Puoi esaminarne le autorizzazioni utilizzando il comando seguente: `kubectl edit configmaps aws-auth --namespace kube-system`

Per revocare l'accesso di un AWS ConfigMap utente:

1. Utilizzate il seguente comando per aprire. ConfigMap

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifica il ruolo o la voce utente nella sezione `MapRoles` o `MapUsers` con lo stesso nome utente riportato nella sezione dei dettagli utente di Kubernetes del tuo risultato. GuardDuty Consulta l'esempio seguente, in cui l'utente amministratore è stato identificato in un esito.

```

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. Rimuovi quell'utente da. ConfigMap Consulta l'esempio seguente, in cui l'utente amministratore è stato rimosso.

```

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. Se il userType è un Utente o un Ruolo assunto da un utente:
 - a. [Ruota la chiave di accesso](#) dell'utente.
 - b. Ruota tutti i segreti a cui l'utente ha avuto accesso.

- c. Controlla le informazioni in [Il mio AWS account potrebbe essere compromesso](#) per ulteriori dettagli.

Se l'esito non ha una sezione `resource.accessKeyDetails`, l'utente è un account di servizio Kubernetes.

Account di servizio: l'account di servizio fornisce un'identità per i pod e può essere identificato da un nome utente con il formato seguente:
`system:serviceaccount:namespace:service_account_name`.

Per revocare l'accesso a un account di servizio:

1. Ruota le credenziali dell'account di servizio.
2. Consulta le linee guida sulla compromissione dei pod nella sezione seguente.

Riparazione dei pod Kubernetes potenzialmente compromessi

Quando si GuardDuty specificano i dettagli di un pod o di una risorsa di carico di lavoro all'interno della `resource.kubernetesDetails.kubernetesWorkloadDetails` sezione, quel pod o risorsa del carico di lavoro è stato potenzialmente compromesso. Un GuardDuty risultato può indicare che un singolo pod è stato compromesso o che più pod sono stati compromessi a causa di una risorsa di livello superiore. Consulta i seguenti scenari di compromissione per indicazioni su come identificare il pod o i pod che sono stati compromessi.

Compromissione di pod singoli

Se il campo `type` all'interno della sezione `resource.kubernetesDetails.kubernetesWorkloadDetails` è `pod`, l'esito identifica un singolo pod. Il campo `nome` è il nome del pod e il campo `namespace` è il relativo spazio del nome.

Per informazioni sull'identificazione del nodo di lavoro che esegue i pod, consulta [Identify the offending pod e worker node](#) nella Amazon EKS Best Practices Guide.

Pod compromessi tramite una risorsa del carico di lavoro

Se il campo `type` all'interno della sezione `resource.kubernetesDetails.kubernetesWorkloadDetails` identifica una Risorsa del carico di lavoro, ad esempio un `Deployment`, è probabile che tutti i pod all'interno della risorsa del carico di lavoro siano stati compromessi.

Per informazioni sull'identificazione di tutti i pod della risorsa del carico di lavoro e dei nodi su cui sono in esecuzione, consulta [Identifica i pod e i nodi di lavoro offensivi utilizzando il nome del carico di lavoro nella](#) Amazon EKS Best Practices Guide.

I pod sono stati compromessi tramite un account di servizio

Se un GuardDuty risultato identifica un account di servizio nella `resource.kubernetesDetails.kubernetesUserDetails` sezione, è probabile che i pod che utilizzano l'account di servizio identificato siano compromessi. Il nome utente riportato da un esito è un account di servizio se ha il formato seguente:
`system:serviceaccount:namespace:service_account_name`.

Per informazioni sull'identificazione di tutti i pod che utilizzano l'account di servizio e i nodi su cui sono in esecuzione, consulta [Identifica i pod e i nodi di lavoro offensivi utilizzando il nome dell'account di servizio](#) nella Amazon EKS Best Practices Guide.

Dopo aver identificato tutti i pod compromessi e i nodi su cui sono in esecuzione, consulta [Isolare il pod creando una politica di rete che neghi tutto il traffico in ingresso e in uscita verso il pod nella](#) Amazon EKS Best Practices Guide.

Per rimediare a un pod potenzialmente compromesso:

1. Identifica la vulnerabilità che ha compromesso i pod.
2. Implementa la correzione di tale vulnerabilità e avvia nuovi pod sostitutivi.
3. Eliminare i pod vulnerabili.

Per ulteriori informazioni, consulta [Redeploy pod o workload compromessi nella](#) Amazon EKS Best Practices Guide.

Se al nodo di lavoro è stato assegnato un ruolo IAM che consente ai Pods di accedere ad altre AWS risorse, rimuovi tali ruoli dall'istanza per evitare ulteriori danni causati dall'attacco. Allo stesso modo, se al pod è stato assegnato un ruolo IAM, valuta se puoi rimuovere in sicurezza le policy IAM dal ruolo senza influire sugli altri carichi di lavoro.

Riparazione delle immagini dei container potenzialmente compromesse

Quando un GuardDuty risultato indica una compromissione del pod, l'immagine utilizzata per avviare il pod potrebbe essere potenzialmente dannosa o compromessa.

GuardDuty i risultati identificano l'immagine del contenitore all'interno del `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Puoi determinare se l'immagine è dannosa scansionandola alla ricerca di malware.

Per correggere un'immagine del contenitore potenzialmente compromessa:

1. Interrompi immediatamente l'utilizzo dell'immagine e rimuovila dal tuo repository di immagini.
2. Identifica tutti i pod utilizzando l'immagine potenzialmente compromessa.

Per ulteriori informazioni, consulta [Identifica i pod con immagini e nodi di lavoro vulnerabili o compromessi](#) nella Amazon EKS Best Practices Guide.

3. Isola i pod potenzialmente compromessi, ruota le credenziali e raccogli dati per l'analisi. Per ulteriori informazioni, consulta [Isolare il pod creando una policy di rete che neghi tutto il traffico in ingresso e in uscita verso il pod nella](#) Amazon EKS Best Practices Guide.
4. Elimina tutti i pod utilizzando l'immagine potenzialmente compromessa.

Riparazione dei nodi Kubernetes potenzialmente compromessi

Un GuardDuty risultato può indicare una compromissione del nodo se l'utente identificato nel risultato rappresenta l'identità di un nodo o se il risultato indica l'uso di un contenitore privilegiato.

L'identità utente è un nodo worker se il campo nome utente ha il seguente formato:

`system:node:node name`. Ad esempio, `system:node:ip-192-168-3-201.ec2.internal`. Ciò indica che l'avversario ha ottenuto l'accesso al nodo e ne utilizza le credenziali per comunicare con l'endpoint dell'API Kubernetes.

Un esito indica l'uso di un container privilegiato se il campo

`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext` dell'esito di uno o più container elencati nell'esito è impostato su `True`.

Per riparare un nodo potenzialmente compromesso:

1. Isola il pod, ruota le sue credenziali e raccogli dati per l'analisi forense.

Per ulteriori informazioni, consulta [Isolare il pod creando una policy di rete che neghi tutto il traffico in ingresso e in uscita verso il pod nella](#) Amazon EKS Best Practices Guide.

2. Identifica gli account di servizio utilizzati da tutti i pod in esecuzione sul nodo potenzialmente compromesso. Controlla le relative autorizzazioni e, se necessario, ruota gli account di servizio.

3. Termina il nodo potenzialmente compromesso.

Riparazione degli esiti del monitoraggio del runtime

Quando abiliti il Runtime Monitoring per il tuo account, Amazon GuardDuty potrebbe generare dati [GuardDuty Tipi di risultati del monitoraggio del runtime](#) che indicano potenziali problemi di sicurezza nel tuo AWS ambiente. I potenziali problemi di sicurezza indicano un'istanza Amazon EC2 compromessa, un carico di lavoro di container, un cluster Amazon EKS o un set di credenziali compromesse nel tuo ambiente. AWS L'agente di sicurezza monitora gli eventi di runtime da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli di ricerca generati nella GuardDuty console. La sezione seguente descrive le procedure di correzione consigliate per ogni tipo di risorsa.

Instance

Se il Tipo di risorsa nei dettagli dell'esito è Istanza, significa che un'istanza EC2 o un nodo EKS sono potenzialmente compromessi.

- Per correggere un nodo EKS compromesso, consulta [Riparazione dei nodi Kubernetes potenzialmente compromessi](#).
- Per correggere un'istanza EC2 compromessa, consulta [Correzione di un'istanza Amazon EC2 potenzialmente compromessa](#).

EKSCluster

Se il tipo di risorsa nei dettagli del risultato è EKSCluster, indica che un pod o un contenitore all'interno di un cluster EKS è potenzialmente compromesso.

- Per correggere un pod compromesso, consulta [Riparazione dei pod Kubernetes potenzialmente compromessi](#).
- Per correggere l'immagine di un container compromessa, consulta [Riparazione delle immagini dei container potenzialmente compromesse](#).

ECSCluster

Se il tipo di risorsa nei dettagli del risultato è ECSCluster, indica che un'attività ECS o un contenitore all'interno di un'attività ECS è potenzialmente compromessa.

1. Identifica il cluster ECS interessato

Il risultato del GuardDuty Runtime Monitoring fornisce i dettagli del cluster ECS nel pannello dei dettagli del risultato o nella `resource.ecsClusterDetails` sezione del JSON di ricerca.

2. Identifica l'attività ECS interessata

Il risultato GuardDuty di Runtime Monitoring fornisce i dettagli dell'attività ECS nel pannello dei dettagli del risultato o nella `resource.ecsClusterDetails.taskDetails` sezione del file JSON di ricerca.

3. Isola l'attività interessata

Isola l'attività interessata bloccando tutto il traffico in entrata e in uscita verso l'attività.

Una regola di blocco totale del traffico può contribuire a fermare un attacco già in corso, interrompendo tutte le connessioni all'attività.

4. Risolvi l'attività compromessa

- a. Identifica la vulnerabilità che ha compromesso l'attività.
- b. Implementa la correzione di tale vulnerabilità e avvia una nuova attività sostitutiva.
- c. Interrompi l'attività vulnerabile.

Container

Se il Tipo di risorsa nei dettagli dell'esito è Container, significa che un container autonomo è potenzialmente compromesso.

- Per procedere alla correzione, consulta [Riparazione di un contenitore autonomo potenzialmente compromesso](#).
- Se l'esito viene generato su più container utilizzando la stessa immagine del container, consulta [Riparazione delle immagini dei container potenzialmente compromesse](#).
- Se il container ha avuto accesso all'host EC2 sottostante, le credenziali dell'istanza associata potrebbero essere state compromesse. Per ulteriori informazioni, consulta [Riparazione delle credenziali potenzialmente compromesse AWS](#).
- Se un attore potenzialmente malintenzionato ha avuto accesso al nodo EKS sottostante o a un'istanza EC2, consulta la soluzione consigliata nelle schede EKSClustere Istanza.

Correzione delle immagini del container compromesse

Quando un GuardDuty risultato indica una compromissione dell'attività, l'immagine utilizzata per avviare l'attività potrebbe essere dannosa o compromessa.

GuardDuty i risultati identificano l'immagine del contenitore all'interno del `resource.ecsClusterDetails.taskDetails.containers.image` campo. È possibile determinare se l'immagine è dannosa o meno eseguendo una scansione alla ricerca di malware.

Per correggere l'immagine compromessa di un contenitore

1. Interrompi immediatamente l'utilizzo dell'immagine e rimuovila dal tuo repository di immagini.
2. Identifica tutte le attività che utilizzano questa immagine.
3. Interrompi tutte le attività che utilizzano l'immagine compromessa. Aggiorna le definizioni delle attività in modo che smettano di utilizzare l'immagine compromessa.

Ripristino di un database potenzialmente compromesso

GuardDuty generi [Tipi di esiti della Protezione RDS](#) che indicano un comportamento di accesso potenzialmente sospetto e anomalo dopo l'attivazione. [Database supportati Protezione RDS](#)

Utilizzando l'attività di accesso RDS, GuardDuty analizza e profila le minacce identificando modelli insoliti nei tentativi di accesso.

Note

Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla [GuardDuty tipi di ricerca attivi](#).

Segui questi passaggi consigliati per correggere un database Amazon Aurora potenzialmente compromesso nel tuo ambiente. AWS

Argomenti

- [Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti](#)
- [Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti](#)
- [Correzione di credenziali potenzialmente compromesse](#)
- [Limita l'accesso alla rete](#)

Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti

I seguenti passaggi consigliati sono utili per correggere un database Aurora potenzialmente compromesso che presenta un comportamento insolito legato a eventi di accesso riusciti.

1. Identifica il database e l'utente interessati.

Il GuardDuty risultato generato fornisce il nome del database interessato e i dettagli utente corrispondenti. Per ulteriori informazioni, consulta [Dettagli degli esiti](#).

2. Verifica se questo comportamento è previsto o non previsto.

L'elenco seguente specifica i potenziali scenari che potrebbero aver causato la generazione GuardDuty di un risultato:

- Un utente che accede al proprio database dopo un lungo periodo di tempo.
- Un utente che accede occasionalmente al proprio database, ad esempio un analista finanziario che accede ogni tre mesi.
- Un attore potenzialmente sospetto coinvolto in un tentativo di accesso riuscito può compromettere il database.

3. Inizia questa fase se il comportamento non è previsto.

1. Limita l'accesso al database

Limita l'accesso al database per gli account sospetti e per l'origine di questa attività di accesso. Per ulteriori informazioni, consultare [Correzione di credenziali potenzialmente compromesse](#) e [Limita l'accesso alla rete](#).

2. Valuta l'impatto e determina a quali informazioni è stato effettuato l'accesso.

- Se disponibili, esamina i log di audit per identificare le informazioni a cui potrebbe essere stato effettuato l'accesso. Per ulteriori informazioni, consulta [Monitoraggio di eventi, registri e flussi in un cluster di database Amazon Aurora](#) nella Guida per l'utente di Amazon Aurora.
- Determina se sono stati effettuati accessi o modifiche a informazioni sensibili o protette.

Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti

I seguenti passaggi consigliati sono utili per correggere un database Aurora potenzialmente compromesso che presenta un comportamento insolito legato a eventi di accesso falliti.

1. Identifica il database e l'utente interessati.

Il GuardDuty risultato generato fornisce il nome del database interessato e i dettagli utente corrispondenti. Per ulteriori informazioni, consulta [Dettagli degli esiti](#).

2. Identifica l'origine dei tentativi di accesso falliti.

Il GuardDuty risultato generato fornisce l'indirizzo IP e l'organizzazione ASN (se si trattava di una connessione pubblica) nella sezione Attore del pannello di ricerca.

Un sistema autonomo (AS) è un gruppo di uno o più prefissi IP (elenchi di indirizzi IP accessibili su una rete) gestiti da uno o più operatori di rete che mantengono un'unica policy di instradamento chiaramente definita. Gli operatori di rete necessitano di Autonomous System Numbers (ASNs) per controllare il routing all'interno delle loro reti e scambiare informazioni di routing con altri provider di servizi Internet (). ISPs

3. Verifica che questo comportamento non sia previsto.

Verifica nel modo seguente se questa attività rappresenta un tentativo di ottenere un ulteriore accesso non autorizzato al database:

- Se l'origine è interna, verifica se un'applicazione non è configurata correttamente e tenta ripetutamente di stabilire una connessione.
- Se si tratta di un attore esterno, verificate se il database corrispondente è pubblico o non correttamente configurato, permettendo così ai potenziali utenti malintenzionati di usare la forza bruta con nomi utente comuni.

4. Inizia questa fase se il comportamento non è previsto.

1. Limita l'accesso al database

Limita l'accesso al database per gli account sospetti e per l'origine di questa attività di accesso. Per ulteriori informazioni, consultare [Correzione di credenziali potenzialmente compromesse](#) e [Limita l'accesso alla rete](#).

2. Esegui l'analisi delle cause principali e determina i passaggi che potenzialmente hanno portato a questa attività.

Imposta un avviso per ricevere una notifica quando un'attività modifica una policy di rete e crea uno stato di insicurezza. Per ulteriori informazioni, consulta [Policy del firewall in AWS Network Firewall](#) nella Guida per gli sviluppatori di AWS Network Firewall .

Correzione di credenziali potenzialmente compromesse

Un GuardDuty risultato può indicare che le credenziali dell'utente per un database interessato sono state compromesse quando l'utente identificato nel risultato ha eseguito un'operazione imprevista sul database. Puoi identificare l'utente nella sezione dei Dettagli utente del database RDS all'interno del pannello dell'esito nella console o all'interno dei `resource.rdsDbUserDetails` del file JSON degli esiti. Questi dettagli utente includono il nome utente, l'applicazione utilizzata, il database a cui si accede, la versione SSL e il metodo di autenticazione.

- Per revocare l'accesso o ruotare le password per utenti specifici coinvolti nell'esito, consulta [Sicurezza con Amazon Aurora MySQL](#) o [Sicurezza con Amazon Aurora PostgreSQL](#) nella Guida per l'utente di Amazon Aurora.
- Utilizzalo Gestione dei segreti AWS per archiviare in modo sicuro e ruotare automaticamente i segreti per i database Amazon Relational Database Service (RDS). Per ulteriori informazioni, consulta [Tutorial di Gestione dei segreti AWS](#) nella Guida per l'utente di Gestione dei segreti AWS .
- Utilizza l'autenticazione del database IAM per gestire l'accesso degli utenti del database senza bisogno di password. Per ulteriori informazioni, consulta [Autenticazione database IAM](#) nella Guida per l'utente di Amazon Aurora.

Per ulteriori informazioni, consulta [Best practice di sicurezza per Amazon Relational Database Service](#) nella Guida per l'utente di Amazon RDS.

Limita l'accesso alla rete

Un GuardDuty risultato può indicare che un database è accessibile oltre le applicazioni o il Virtual Private Cloud (VPC). Se l'indirizzo IP remoto indicato nell'esito è un'origine di connessione non prevista, controlla i gruppi di sicurezza. Un elenco dei gruppi di sicurezza collegati al database è disponibile in Gruppi **resource.rdsDbInstanceDetails.dbSecurityGroups** di sicurezza nella <https://console.aws.amazon.com/rds/console> o nei risultati JSON. Per maggiori informazioni sulla

configurazione dei gruppi di sicurezza, consulta [Controllo dell'accesso con i gruppi di sicurezza](#) nella Guida dell'utente di Amazon RDS.

Se utilizzi un firewall, limita l'accesso alla rete al database riconfigurando le liste di controllo degli accessi alla rete (). NACLs Per ulteriori informazioni, consulta [Firewall in AWS Network Firewall](#) nella Guida per gli sviluppatori di AWS Network Firewall .

Correzione di una funzione Lambda potenzialmente compromessa

Quando viene GuardDuty generata [Tipi di esiti della Protezione Lambda](#), la funzione Lambda potrebbe essere compromessa. Se l'attività che ha causato la generazione GuardDuty di questo risultato era prevista, puoi prendere in considerazione l'utilizzo. [Regole di eliminazione](#) Ti consigliamo di completare i seguenti passaggi per correggere una funzione Lambda compromessa:

Per correggere gli esiti della Protezione Lambda

1. Identifica la versione della funzione Lambda potenzialmente compromessa.

Un GuardDuty risultato di Lambda Protection fornisce il nome, Amazon Resource Name (ARN), la versione della funzione e l'ID di revisione associati alla funzione Lambda elencati nei dettagli del risultato.

2. Identifica l'origine dell'attività potenzialmente sospetta.

- a. Esamina il codice associato alla versione della funzione Lambda coinvolta nell'esito.
- b. Esamina le librerie importate e i livelli della versione della funzione Lambda coinvolta nell'esito.
- c. Se hai abilitato [AWS Lambda le funzioni di scansione con Amazon Inspector](#), esamina i risultati di [Amazon Inspector associati](#) alla funzione Lambda coinvolta nel risultato.
- d. AWS CloudTrail Esamina i log per identificare la causa principale che ha causato l'aggiornamento della funzione e assicurati che l'attività sia stata autorizzata o prevista.

3. Correggi la funzione Lambda potenzialmente compromessa.

- a. Disabilita i trigger di esecuzione della funzione Lambda coinvolta nell'esito. Per ulteriori informazioni, consulta [DeleteFunctionEventInvokeConfig](#).
- b. Esamina il codice Lambda e aggiorna le importazioni delle librerie e i [Livelli della funzione Lambda](#) per rimuovere le librerie e i livelli potenzialmente sospetti.
- c. Contieni gli esiti di Amazon Inspector relativi alla funzione Lambda coinvolta nell'esito.

Monitoraggio GuardDuty dell'utilizzo e stima dei costi

GuardDuty fornisce metriche di utilizzo che tracciano l'elaborazione dei piani di protezione, delle fonti di dati logs/events e del GuardDuty Runtime, monitorati VCPUs nel tempo.

In questa pagina:

- [Metriche CloudWatch di utilizzo di Amazon](#)
- [Comprensione dell'utilizzo GuardDuty](#)
- [GuardDuty Stima dei costi](#)

Metriche CloudWatch di utilizzo di Amazon

GuardDuty pubblica i parametri di utilizzo su Amazon CloudWatch, consentendoti di:

- Tieni traccia dell'utilizzo effettivo nel tempo
- Crea dashboard e allarmi personalizzati
- Esporta i dati di utilizzo per la stima dei costi in Pricing Calculator AWS

GuardDuty le metriche di utilizzo sono pubblicate in base alla configurazione dell'account:

- Per gli account autonomi (che non fanno parte di un'organizzazione), puoi visualizzare le metriche di utilizzo del tuo account in Amazon CloudWatch
- Per gli account che fanno parte di un'organizzazione, le metriche vengono pubblicate nell'account amministratore delegato (GuardDuty amministratore dell'organizzazione), che presenta l'utilizzo aggregato per l'intera organizzazione

GuardDuty le metriche di utilizzo vengono pubblicate su Amazon CloudWatch entro 24 ore.

Dettagli metrici

GuardDuty pubblica le seguenti metriche di utilizzo Hourly su Amazon nel CloudWatch AWS/GuardDuty namespace:

Piano di protezione	Origine dati	Nome parametro	Unità	Descrizione
Rilevamento delle minacce di base	CloudTrailEvents	AnalyzedCount	Conteggio	Numero di eventi di CloudTrail gestiti e analizzati
Rilevamento delle minacce di base	VPCFlowRe gistra eventi DNSLog	AnalyzedBytes	Byte	Volume dei log di flusso VPC e dei log DNS analizzati
Protezione EKS	Kubernete sAuditLogs	AnalyzedCount	Conteggio	Numero di eventi del registro di controllo di Amazon EKS analizzati
Protezione S3	S3 DataEvents	AnalyzedCount	Conteggio	Numero di eventi relativi ai dati S3 analizzati
Monitoraggio del runtime	RuntimeMo nitoringEC2	Monitored VcpuHours	Conteggio (ore- vCPU)	Ore di vCPU EC2 monitorate da Runtime Monitoring
Monitoraggio del runtime	RuntimeMo nitoringEKS	Monitored VcpuHours	Conteggio (ore- vCPU)	Ore di vCPU Amazon EKS monitorate da Runtime Monitoring
Monitoraggio del runtime	RuntimeMo nitoringFargate	Monitored VcpuHours	Conteggio (ore- vCPU)	Ore di vCPU Fargate monitorate

				da Runtime Monitoring
Protezione da malware per EC2	OnDemandEBSSnapshot	ScannedBytes	Byte	Volume di dati di snapshot EBS su richiesta scansionati
Protezione da malware per EC2	OnDemandEBSVolume	ScannedBytes	Byte	Volume di dati di volume EBS su richiesta scansionati
Protezione da malware per EC2	MalwareProtectionEBS	ScannedBytes	Byte	Volume di dati EBS scansionati da Malware Protection
Protezione RDS	RDS	MonitoredAcuHours	Conteggio (ore ACU)	Unità di capacità Amazon RDS Aurora monitorate
Protezione RDS	RDSLimitless	MonitoredAcuHours	Conteggio (ore ACU)	Monitoraggio delle ore ACU di Amazon RDS Aurora Limitless
Protezione RDS	AuroraScaleout	MonitoredAcuHours	Conteggio (ore ACU)	Monitoraggio delle ore dell'unità ACU Aurora Scaleout
Protezione RDS	RDS	MonitoredVcpuHours	Conteggio (ore-vCPU)	Monitoraggio delle ore di vCPU di Amazon RDS

Protezione Lambda	LambdaNet workLogs	AnalyzedBytes	Byte	Volume di log di rete Lambda analizzati

Metriche e dimensioni

- GuardDuty Account autonomi: le metriche includono le dimensioni AccountId, DataSource
- A livello di organizzazione (amministratore delegato): le metriche includono la dimensione DataSource

Protezione da malware per S3

GuardDuty Malware Protection for S3 il piano di protezione pubblica le seguenti metriche di utilizzo su Amazon nello spazio dei CloudWatch AWS/GuardDuty/MalwareProtection nomi:

Nome parametro	Unità	Descrizione
CompletedScanCount	Conteggio	Il numero di scansioni antimalware di oggetti S3 completate in un determinato periodo di tempo.
FailedScanCount	Conteggio	Il numero di scansioni di malware relative agli oggetti S3 che non sono riuscite in un determinato periodo di tempo.
SkippedScanCount	Conteggio	Il numero di scansioni di malware relative agli oggetti S3 che sono state ignorate in un determinato periodo di tempo.
InfectedScanCount	Conteggio	Il numero di scansioni di malware relative agli oggetti S3 che hanno rilevato oggetti

potenzialmente dannosi in un determinato periodo di tempo.

CompletedScanBytes	Conteggio	Il numero di byte di oggetti S3 scansionati in un determinato periodo di tempo.

Metriche e dimensioni

- Tutte le metriche includono le dimensioni Malware Protection Plan Id, Resource Name
- SkippedScanCount la metrica include Skipped Reason come dimensione aggiuntiva

Comprensione dell'utilizzo GuardDuty

GuardDuty Elaborazione degli eventi

Se abilitata, consuma GuardDuty automaticamente gli eventi e i log direttamente dalle sorgenti di registro selezionate. Regione AWS GuardDuty inserisce eventi da fonti di dati separate e indipendenti per fornire un valore di sicurezza completo.

Important

La configurazione individuale dei log di servizio o le regole di filtraggio (per i log di flusso VPC, i registri DNS, gli eventi, gli eventi di dati S3 CloudTrail, i registri di controllo Kubernetes e i registri di rete Lambda) non influiscono sull'elaborazione da logs/events GuardDuty

GuardDuty Costi di elaborazione dei log di flusso VPC per le istanze monitorate da Runtime Monitoring GuardDuty

[Per le istanze monitorate da GuardDuty Runtime Monitoring \(tramite l'agente EC2 Runtime o l'agente Amazon EKS Runtime\), non GuardDuty verrà addebitato alcun costo per l'elaborazione dei log di flusso VPC purché l'agente invii attivamente i dati degli eventi di runtime.](#) Se l'agente interrompe la trasmissione dei dati degli eventi, GuardDuty torna alla ricarica tramite VPC Flow Logs.

L'abilitazione del Runtime Monitoring riduce l'utilizzo dei VPC Flow Logs nelle metriche di utilizzo di GuardDuty Amazon CloudWatch . La disabilitazione del Runtime Monitoring ripristina l'utilizzo dei log di flusso VPC.

GuardDuty Stima dei costi

GuardDuty offre una prova gratuita di 30 giorni per AWS account per la maggior parte dei piani di protezione. Durante questo periodo di prova, puoi:

- Monitora il tuo utilizzo effettivo tramite le metriche GuardDuty di utilizzo
- Stima i costi mensili utilizzando AWS Pricing Calculator in base ai modelli di utilizzo osservati

I seguenti piani di protezione includono una prova gratuita di 30 giorni:

- Rilevamento delle minacce di base
- Protezione S3
- Protezione EKS
- Monitoraggio del runtime
- Protezione RDS
- Protezione Lambda
- Protezione da malware per EC2 (solo per le scansioni GuardDuty avviate se abilitata con Foundational Threat Detection)

Clienti Security Hub

Security Hub offre un modello di prezzo semplificato per il rilevamento delle GuardDuty minacce con il suo piano aggiuntivo Threat Analytics, che consolida la misurazione di più dati. GuardDuty DataSources Quando si utilizza il piano Security Hub Threat Analytics (Security Hub con GuardDuty):

- Molteplici GuardDuty DataSources sono consolidati
- In particolare, per semplicità, gli eventi di Amazon EKS Audit Logs e gli eventi S3 Data vengono convertiti in GB utilizzando un tasso di conversione fisso

Per creare una stima dei costi di Security Hub, consulta la [documentazione di AWS Security Hub](#).

Nota: lo stato GuardDuty della prova gratuita di 30 giorni è indipendente dall'integrazione con Security Hub. Attivazione o disattivazione del Security Hub:

- Non concede una nuova prova gratuita se hai già utilizzato il periodo GuardDuty di prova
- Non interrompe o riavvia una prova gratuita in corso
- Non prolunga i periodi di prova esistenti

Nomi delle funzionalità per i piani di protezione nell' GuardDuty API

Quando abiliti Amazon GuardDuty per la prima volta, inizia l'elaborazione [Origini dati fondamentali](#) all'interno del tuo AWS ambiente. GuardDuty utilizza queste fonti di dati per elaborare un flusso indipendente di eventi come log di flusso VPC, log DNS ed eventi di gestione. AWS CloudTrail Successivamente analizza questi eventi per identificare potenziali minacce alla sicurezza e genera esiti nel tuo account.

Quando uno o più piani di protezione sono abilitati, GuardDuty utilizza dati aggiuntivi provenienti da altri AWS servizi AWS dell'ambiente per monitorare e analizzare potenziali minacce alla sicurezza. Queste fonti di dati aggiuntive sono chiamate funzionalità.

Passaggio dalle fonti di dati alle funzionalità

Quando aggiungi GuardDuty protezioni aggiuntive, come S3 Protection, Runtime Monitoring, Lambda Protection e altre, puoi configurare la GuardDuty funzionalità corrispondente al piano di protezione. Storicamente, le GuardDuty protezioni venivano chiamate in. `dataSources` APIs Tuttavia, dopo marzo 2023, i nuovi piani di GuardDuty protezione sono ora configurati così `features` e non. `dataSources` GuardDuty supporta ancora la configurazione dei piani di protezione lanciati prima di marzo 2023, come `dataSources` tramite l'API, ma i nuovi piani di protezione sono disponibili solo come `features`. Per informazioni sui piani di protezione interessati, consulta. [GuardDuty Modifiche all'API](#)

Se gestisci i piani di GuardDuty configurazione e protezione tramite la console, non sei direttamente interessato da questa modifica e non devi intraprendere alcuna azione. Questa modifica influisce sul comportamento di coloro APIs che vengono richiamati per abilitare GuardDuty o sui piani di protezione all'interno. GuardDuty Se si utilizza APIs o si AWS CLI desidera abilitare o modificare la configurazione di un piano di protezione, è necessario utilizzare il nome della funzionalità associata. Per ulteriori informazioni, consulta [Mappatura di dataSources su features](#).

GuardDuty Modifiche all'API a marzo 2023

GuardDuty APIs Configurano le funzionalità di protezione che non appartengono all'elenco di [GuardDuty fonti di dati fondamentali](#). Un oggetto `feature` contiene dettagli sulle funzionalità, come

il nome e lo stato della funzionalità, e può contenere configurazioni aggiuntive per alcuni piani di protezione. Questa migrazione influisce su quanto segue APIs nell'Amazon GuardDuty API Reference:

- [CreateDetector](#)
- [GetDetector](#)
- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

Funzionalità rispetto alle fonti di dati

Storicamente, tutte le GuardDuty funzionalità venivano trasmesse attraverso un `dataSources` oggetto nell'API. A partire da marzo 2023, GuardDuty preferisce `features` l'oggetto anziché l'`dataSources` oggetto nell'API. Tutte le origini dati precedenti hanno funzionalità corrispondenti, ma le funzionalità più recenti potrebbero non avere origini dati corrispondenti.

L'elenco seguente mostra il confronto tra l'oggetto `dataSources` e l'oggetto `features` quando viene trasmesso tramite un'API:

- L'oggetto `dataSources` contiene oggetti per ogni tipo di protezione e il relativo stato. L'`features` oggetto è un elenco di funzionalità disponibili che corrispondono a ciascun tipo di protezione all'interno GuardDuty.

A partire da marzo 2023, l'attivazione delle funzionalità sarà l'unico modo per configurare nuove GuardDuty funzionalità nel proprio AWS ambiente.

- Lo `dataSources` schema nella richiesta o nella risposta dell'API è lo stesso in tutti i paesi in Regione AWS cui GuardDuty è disponibile. Tuttavia, è possibile che non tutte le funzionalità siano disponibili in ogni regione. Pertanto, i nomi delle funzionalità disponibili possono variare in base alla regione.

Capire come funzionano APIs le funzionalità

GuardDuty APIs Continueranno a restituire un `dataSources` oggetto, se applicabile, e restituiranno anche un `features` oggetto contenente le stesse informazioni in un formato diverso. GuardDuty le funzionalità lanciate prima di marzo 2023 saranno disponibili tramite `dataSources` object and `features` object. GuardDuty le funzionalità lanciate a partire da marzo 2023 saranno disponibili solo tramite l'`features` oggetto. Non è possibile creare o aggiornare un rilevatore o descrivere AWS Organizations l'utilizzo di entrambi `dataSources` e della notazione `features` degli oggetti nella stessa richiesta API. Per abilitare i tipi di GuardDuty protezione, dovrai migrare le fonti di dati esistenti `features` sull'oggetto utilizzando le stesse APIs che ora includono anche l'`features` oggetto.

Note

GuardDuty non aggiungerà una nuova fonte di dati dopo questa modifica.

GuardDuty ha reso obsoleto l'uso di fonti di dati associate ai piani di protezione. Tuttavia, supporta ancora le [GuardDuty fonti di dati fondamentali](#). Le GuardDuty migliori pratiche consigliano di utilizzare funzionalità per abilitare o modificare la configurazione di qualsiasi piano di protezione del proprio account.

Incorporazione delle modifiche alle funzionalità in APIs

- Se gestisci GuardDuty le configurazioni tramite APIs o CloudFormation modello e desideri abilitare potenziali nuove GuardDuty funzionalità, dovrai modificare rispettivamente il codice e il modello. SDKs Per ulteriori informazioni, consulta l'aggiornamento APIs nell'[Amazon GuardDuty API Reference](#).
- Per GuardDuty le funzionalità configurate prima di questo aggiornamento, puoi continuare a utilizzare il CloudFormation modello APIs SDKs, o. Tuttavia, ti consigliamo di passare all'utilizzo dell'oggetto `feature`.

Tutte le origini dati hanno un oggetto funzionalità equivalente. Per ulteriori informazioni, consulta [Mappatura di `dataSources` su `features`](#).

- Attualmente, la `additionalConfiguration` nell'oggetto `features` è disponibile solo per determinati tipi di protezione.

- Per questi tipi di protezione, se la funzionalità `AdditionalConfiguration status` è impostata su `ENABLED` ma la configurazione della funzionalità non `status` è impostata su `ENABLED`, non GuardDuty intraprenderà alcuna azione in questo caso.
- Ciò influisce APIs su quanto segue:
 - [UpdateDetector](#)
 - [UpdateMemberDetectors](#)
 - [UpdateOrganizationConfiguration](#)

Mappatura di **dataSources** su **features**

La tabella seguente mostra la mappatura dei tipi di protezione, delle `dataSources` e delle `features`.

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Log di flusso VPC	<code>flowLogs</code> (sola lettura; non possono essere modificati)	<code>FLOW_LOGS</code> (sola lettura; non possono essere modificati)
Registri delle query DNS di Route53 Resolver	<code>dnsLogs</code> (sola lettura; non possono essere modificati)	<code>DNS_LOGS</code> (sola lettura; non possono essere modificati)
CloudTrail eventi	<code>cloudTrail</code> (sola lettura; non possono essere modificati)	<code>CLOUD_TRAIL</code> (sola lettura; non possono essere modificati)
S3	<code>s3Logs</code>	<code>S3_DATA_EVENTS</code>
Protezione EKS	<code>kubernetes.auditlogs</code>	<code>EKS_AUDIT_LOGS</code>
Protezione da malware per EC2	<code>malwareProtection.scanEc2InstancesWithFindings.ebsVolumes</code>	<code>EBS_MALWARE_PROTECTION</code>

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Eventi di accesso RDS	GuardDuty fornisce solo il supporto per l'attivazione delle funzionalità per questi tipi di protezione.	RDS_LOGIN_EVENTS
Monitoraggio del runtime EKS		EKS_RUNTIME_MONITORING
Monitoraggio del runtime		RUNTIME_MONITORING
GuardDuty agente di sicurezza per cluster Amazon EKS		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
GuardDuty agente di sicurezza per cluster Amazon ECS-Fargate		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
GuardDuty agente di sicurezza per istanze Amazon EC2		RUNTIME_MONITORING_additionalConfiguration.EC2_AGENT_MANAGEMENT
Protezione Lambda		LAMBDA_NETWORK_LOGS

*GetUsageStatistics utilizza i propri nomi di dataSource. Per ulteriori informazioni, consulta [Monitoraggio GuardDuty dell'utilizzo e stima dei costi](#) o [GetUsageStatistics](#).

Sicurezza in Amazon GuardDuty

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il [Modello di responsabilità condivisa](#) descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. Per maggiori informazioni sui programmi di conformità applicabili a GuardDuty, consulta la sezione [AWS Servizi rientranti nell'ambito dei programmi di conformità](#), .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo GuardDuty. Ti mostra come configurare per GuardDuty soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere GuardDuty le tue risorse.

Indice

- [Protezione dei dati in Amazon GuardDuty](#)
- [Registrazione delle chiamate GuardDuty API Amazon con AWS CloudTrail](#)
- [Identity and Access Management per Amazon GuardDuty](#)
- [Convalida della conformità per Amazon GuardDuty](#)
- [Resilienza in Amazon GuardDuty](#)
- [Sicurezza dell'infrastruttura in Amazon GuardDuty](#)
- [Amazon GuardDuty e gli endpoint VPC di interfaccia \(\)AWS PrivateLink](#)

Protezione dei dati in Amazon GuardDuty

Il [modello di responsabilità AWS condivisa](#) di si applica alla protezione dei dati in Amazon GuardDuty. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale

che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori GuardDuty o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati a riposo

Tutti i dati dei GuardDuty clienti vengono crittografati quando sono inattivi utilizzando soluzioni di AWS crittografia.

GuardDuty i dati, come i risultati, vengono crittografati quando sono inattivi utilizzando AWS Key Management Service (AWS KMS) utilizzando chiavi gestite dal cliente di AWS proprietà.

Crittografia dei dati in transito

GuardDuty analizza i dati di registro di altri servizi. e crittografa tutti i dati in transito con HTTPS e KMS. Una volta GuardDuty estratte le informazioni necessarie dai log, queste vengono eliminate. [Per ulteriori informazioni su come GuardDuty utilizza le informazioni di altri servizi, consulta le fonti di dati. GuardDuty](#)

GuardDuty i dati vengono crittografati durante il transito tra i servizi.

Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio

Puoi scegliere di non utilizzare i tuoi dati per sviluppare GuardDuty e migliorare altri servizi di AWS sicurezza utilizzando la politica di AWS Organizations opt-out. Puoi scegliere di rinunciare anche se al momento GuardDuty non raccoglie tali dati. Per ulteriori informazioni in merito, consulta le [Policy di rifiuto dei servizi di IA](#) nella Guida per l'utente di AWS Organizations .

Note

Per poter utilizzare la politica di opt-out, i tuoi AWS account devono essere gestiti centralmente da AWS Organizations. Se non hai ancora creato un'organizzazione per i tuoi AWS account, consulta [Creare e gestire un'organizzazione](#) nella Guida per l'AWS Organizations utente.

Il rifiuto esplicito ha gli effetti seguenti:

- GuardDuty eliminerà i dati raccolti e archiviati per scopi di miglioramento del servizio prima dell'eventuale rinuncia da parte dell'utente.
- Dopo l'annullamento, non GuardDuty raccoglieremo o memorizzeremo più questi dati per scopi di miglioramento del servizio.

I seguenti argomenti spiegano come ciascuna funzionalità all'interno di ciascuna funzionalità gestisca GuardDuty potenzialmente i dati per il miglioramento del servizio.

Indice

- [GuardDuty Monitoraggio del runtime](#)
- [GuardDuty Protezione da malware](#)

GuardDuty Monitoraggio del runtime

GuardDuty Il monitoraggio del runtime fornisce il rilevamento delle minacce in fase di esecuzione solo per i cluster Amazon Elastic Kubernetes Service (Amazon EKS) AWS Fargate , Amazon Elastic Container Service (Amazon ECS) e le istanze Amazon Elastic Compute Cloud (Amazon EC2) nel tuo ambiente. AWS Dopo aver abilitato il Runtime Monitoring e distribuito l'agente di GuardDuty sicurezza per la tua risorsa, GuardDuty inizia a monitorare e analizzare gli eventi di runtime associati alla tua risorsa. Questi tipi di eventi di runtime includono eventi di processo, eventi container, eventi DNS e altro ancora. Per ulteriori informazioni, consulta [Tipi di eventi di runtime raccolti che GuardDuty utilizzano](#).

GuardDuty raccoglie sia i comandi (come `curlsystemctl`, `andcron`) che gli argomenti associati (come `start`, `stop`, `disable`) dai carichi di lavoro. Ad esempio, quando qualcuno viene eseguito `systemctl stop service-name`, GuardDuty acquisisce sia il comando che `systemctl` i relativi argomenti. `stop service-name` Queste informazioni dettagliate aiutano GuardDuty a rilevare minacce sofisticate analizzando i modelli di comando e correlando più eventi. Ad esempio, GuardDuty possono identificare quando un utente malintenzionato tenta di disattivare i servizi di sicurezza o esegue file dannosi noti. Sebbene utilizzi GuardDuty attivamente questi dati per il rilevamento delle minacce, attualmente non utilizza questi comandi e argomenti per scopi di miglioramento del servizio (potrebbe farlo in futuro). La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiamo che il nostro utilizzo rispetta i nostri impegni nei tuoi confronti. Per ulteriori informazioni, consulta le [Domande frequenti sulla privacy dei dati](#).

GuardDuty Protezione da malware

GuardDuty Malware Protection analizza e rileva il malware contenuto nei volumi EBS collegati ai carichi di lavoro di istanze Amazon EC2 e container potenzialmente compromessi, i file appena caricati nei bucket Amazon S3 selezionati e le risorse di backup. Attualmente, GuardDuty non raccoglie né utilizza il malware rilevato per migliorare il servizio. Tuttavia, in futuro, quando

GuardDuty Malware Protection identificherà un file di volume EBS, un file di backup o un file S3 come dannoso o dannoso, GuardDuty Malware Protection raccoglierà e archiverà questo file per sviluppare e migliorare i rilevamenti di malware e il servizio. GuardDuty Questo file può essere utilizzato anche per sviluppare e migliorare altri servizi di sicurezza AWS . La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiamo che il nostro utilizzo rispetta i nostri impegni nei tuoi confronti. Per ulteriori informazioni, consulta le [Domande frequenti sulla privacy dei dati](#).

Registrazione delle chiamate GuardDuty API Amazon con AWS CloudTrail

Amazon GuardDuty è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in GuardDuty. CloudTrail acquisisce tutte le chiamate API relative GuardDuty agli eventi, incluse le chiamate dalla GuardDuty console e le chiamate in codice a. GuardDuty APIs Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per. GuardDuty Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta a cui è stata effettuata GuardDuty, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, incluse le modalità di configurazione e attivazione, consulta la [Guida per l'AWS CloudTrail utente](#).

GuardDuty informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in GuardDuty, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di GuardDuty, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni . Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta:

- [Panoramica della creazione di un percorso](#)
- [Servizi e integrazioni CloudTrail supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali di accesso utente root o utente IAM
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, consulta [Elemento userIdentity di CloudTrail](#).

GuardDuty eventi del piano di controllo in CloudTrail

Per impostazione predefinita, CloudTrail registra tutte le operazioni GuardDuty API fornite in [Amazon GuardDuty API Reference](#) come eventi nei CloudTrail file.

GuardDuty eventi relativi ai dati in CloudTrail

[GuardDuty monitoraggio del runtime](#) utilizza un agente di GuardDuty sicurezza distribuito nei cluster Amazon Elastic Kubernetes Service (Amazon EKS), solo nelle attività Amazon Elastic Compute Cloud (Amazon EC2) e nelle aws-guardduty-agent attività (Amazon Elastic Container Service (AWS Fargate Amazon ECS)) per raccogliere [Tipi di eventi di runtime raccolti](#) componenti aggiuntivi () per i carichi di lavoro e inviarli a rilevamento e analisi delle minacce. AWS GuardDuty

Registrazione e monitoraggio degli eventi di dati

Facoltativamente, puoi configurare i log per visualizzare gli eventi relativi ai dati per il tuo agente di sicurezza. AWS CloudTrail GuardDuty

Per creare e configurare CloudTrail, consulta [Data events](#) nella Guida per l'AWS CloudTrail utente e segui le istruzioni per Logging data events con selettori di eventi avanzati in. Console di gestione AWS Durante la registrazione del trail, assicurati di apportare le modifiche seguenti:

- Per il tipo di evento Data, scegli GuardDuty detector.
- Per il Modello di selettore di log, scegli Registra tutti gli eventi.
- Espandi la Visualizzazione JSON per la configurazione, che dovrebbe essere simile al file JSON seguente:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Dopo aver abilitato il selettore per il percorso, accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/> Puoi scaricare gli eventi relativi ai dati dal bucket S3 scelto al momento della configurazione dei log. CloudTrail

Esempio: voci dei file di registro GuardDuty

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che mostra l'evento del piano dati.

```

{
  "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-EXAMPLEbbbbbb",
  "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'esempio seguente mostra una voce di CloudTrail registro che dimostra l'CreateIPThreatIntelSetazione (evento del piano di controllo).

```

{
  "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"
}
```

Da queste informazioni sull'evento puoi determinare che la richiesta è stata effettuata per creare un elenco di minacce Example in GuardDuty. Puoi inoltre vedere che la richiesta è stata effettuata da un utente denominato Alice il 14 giugno 2018.

Identity and Access Management per Amazon GuardDuty

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. GuardDuty IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come GuardDuty funziona Amazon con IAM](#)
- [Esempi di policy basate sull'identità per Amazon GuardDuty](#)
- [Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty](#)
- [AWS politiche gestite per Amazon GuardDuty](#)
- [Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come GuardDuty funziona Amazon con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [Esempi di policy basate sull'identità per Amazon GuardDuty](#))

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Come GuardDuty funziona Amazon con IAM

Prima di utilizzare IAM per gestire l'accesso a GuardDuty, scopri con quali funzionalità IAM è disponibile l'uso GuardDuty.

Funzionalità IAM che puoi utilizzare con Amazon GuardDuty

Funzionalità IAM	GuardDuty supporto
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale

Funzionalità IAM	GuardDuty supporto
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come GuardDuty e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta [AWS i servizi che funzionano con IAM nella IAM](#) User Guide.

Politiche basate sull'identità per GuardDuty

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per GuardDuty

Per visualizzare esempi di politiche basate sull' GuardDuty identità, vedere. [Esempi di policy basate sull'identità per Amazon GuardDuty](#)

Politiche basate sulle risorse all'interno GuardDuty

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket

Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni politiche per GuardDuty

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento Action di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di GuardDuty azioni, consulta [Azioni definite da Amazon GuardDuty](#) nel Service Authorization Reference.

Le azioni politiche in GuardDuty uso utilizzano il seguente prefisso prima dell'azione:

```
guardduty
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "guardduty:action1",  
    "guardduty:action2"  
]
```

Per visualizzare esempi di politiche GuardDuty basate sull'identità, vedere. [Esempi di policy basate sull'identità per Amazon GuardDuty](#)

Risorse politiche per GuardDuty

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di GuardDuty risorse e relativi ARNs, consulta [Resources defined by Amazon GuardDuty](#) nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta [Azioni definite da Amazon](#). GuardDuty

Per visualizzare esempi di politiche GuardDuty basate sull'identità, consulta [Esempi di policy basate sull'identità per Amazon GuardDuty](#)

Chiavi relative alle condizioni delle politiche per GuardDuty

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco di chiavi di GuardDuty condizione, consulta [Condition keys for Amazon GuardDuty](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Amazon GuardDuty](#).

Per visualizzare esempi di politiche GuardDuty basate sull'identità, consulta [Esempi di policy basate sull'identità per Amazon GuardDuty](#)

Liste di controllo degli accessi () in ACLs GuardDuty

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con GuardDuty

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con GuardDuty

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per

ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per GuardDuty

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per GuardDuty

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere GuardDuty la funzionalità. Modifica i ruoli di servizio solo quando viene GuardDuty fornita una guida in tal senso.

Ruoli collegati ai servizi per GuardDuty

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli GuardDuty collegati ai servizi, consulta [Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty](#)

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta [Servizi AWS supportati da IAM](#). Trova un servizio nella tabella che include un Yes nella colonna Service-linked

role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon GuardDuty

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse GuardDuty. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da GuardDuty, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per Amazon GuardDuty](#) nel Service Authorization Reference.

Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console GuardDuty](#)
- [Autorizzazioni necessarie per l'attivazione GuardDuty](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Policy IAM personalizzata per concedere l'accesso in sola lettura a GuardDuty](#)
- [Negare l'accesso ai risultati GuardDuty](#)
- [Utilizzo di una policy IAM personalizzata per limitare l'accesso alle GuardDuty risorse](#)

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare GuardDuty risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti

specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo della console GuardDuty

Per accedere alla GuardDuty console Amazon, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle GuardDuty risorse del tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la GuardDuty console, allega anche la policy GuardDuty ConsoleAccess o la policy ReadOnly AWS gestita alle entità. Per maggiori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente di IAM.

Autorizzazioni necessarie per l'attivazione GuardDuty

Per concedere le autorizzazioni necessarie a diverse identità IAM (utenti, gruppi e ruoli), allega la [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#) policy di attivazione richiesta. GuardDuty

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando l'API or a livello di codice. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
```

```

        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Policy IAM personalizzata per concedere l'accesso in sola lettura a GuardDuty

Per concedere l'accesso in sola lettura GuardDuty puoi utilizzare la policy gestita.

AmazonGuardDutyReadOnlyAccess

Per creare una policy personalizzata che conceda l'accesso in sola lettura a un ruolo, un utente o un gruppo IAM GuardDuty, puoi utilizzare la seguente dichiarazione:

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": "*"
}
]
}

```

Negare l'accesso ai risultati GuardDuty

Puoi utilizzare la seguente policy per negare a un ruolo, utente o gruppo IAM l'accesso ai GuardDuty risultati. Gli utenti non possono visualizzare i risultati o i dettagli sui risultati, ma possono accedere a tutte le altre GuardDuty operazioni:

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"
}
]
}

```

Utilizzo di una policy IAM personalizzata per limitare l'accesso alle GuardDuty risorse

Per definire l'accesso di un utente in GuardDuty base all'ID del rilevatore, puoi utilizzare tutte le [azioni GuardDuty API](#) nelle tue policy IAM personalizzate, ad eccezione delle seguenti operazioni:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty>DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Utilizza le seguenti operazioni in una policy IAM per definire l'accesso di un utente a in GuardDuty base all' IPSet ID e all' ThreatIntelSet ID:

- `guardduty>DeleteIPSet`
- `guardduty>DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

I seguenti esempi mostrano come creare delle policy utilizzando alcune delle operazioni precedenti:

- Questa policy consente a un utente di eseguire l'operazione `guardduty:UpdateDetector` utilizzando l'ID rilevatore 1234567 nella regione us-east-1:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector"
      ],

```

```

    "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567"
  }
]
}

```

- Questo criterio consente a un utente di eseguire l'`guardduty:UpdateIPSet` operazione, utilizzando l'ID del rilevatore 1234567 e l' IPSet ID 000000 nella regione us-east-1:

Note

Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta [Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/000000"
    }
  ]
}

```

- Questo criterio consente a un utente di eseguire l'`guardduty:UpdateIPSet` operazione, utilizzando qualsiasi ID del rilevatore e l' IPSet ID 000000 nella regione us-east-1:

Note

Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta [Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/ipset/000000"
    }
  ]
}
```

- Questa politica consente a un utente di eseguire l'guardduty:UpdateIPSet operazione, utilizzando il proprio ID del rilevatore e qualsiasi IPSet ID nella regione us-east-1:

 Note

Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in GuardDuty. Per ulteriori informazioni, consulta [Impostazione dei prerequisiti per gli elenchi di entità e gli elenchi di indirizzi IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/ipset/*"
    }
  ]
}
```

}

Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty

Amazon GuardDuty utilizza ruoli [collegati ai servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato al servizio (SLR) è un tipo unico di ruolo IAM a cui è collegato direttamente. GuardDuty I ruoli collegati ai servizi sono predefiniti GuardDuty e includono tutte le autorizzazioni necessarie per chiamare altri servizi per GuardDuty tuo conto. AWS

Con il ruolo collegato al servizio, puoi eseguire la configurazione GuardDuty senza aggiungere manualmente le autorizzazioni necessarie. GuardDuty definisce le autorizzazioni del suo ruolo collegato al servizio e, a meno che le autorizzazioni non siano definite diversamente, solo può assumere il ruolo. GuardDuty Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

GuardDuty supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui è disponibile. GuardDuty Per ulteriori informazioni, consulta [Regioni ed endpoint](#).

È possibile eliminare il ruolo GuardDuty collegato al servizio solo dopo la prima disabilitazione GuardDuty in tutte le regioni in cui è abilitato. In questo modo proteggi GuardDuty le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedervi.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) nella Guida per l'utente IAM e cerca i servizi che riportano Sì nella colonna Ruoli collegati ai servizi. Scegliere Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate al servizio per GuardDuty

GuardDuty utilizza il ruolo collegato al servizio (SLR) denominato. `AWSServiceRoleForAmazonGuardDuty` La SLR consente di GuardDuty eseguire le seguenti attività. Consente inoltre di GuardDuty includere i metadati recuperati appartenenti all'istanza EC2 nei risultati che GuardDuty possono generare sulla potenziale minaccia. Ai fini dell'assunzione del ruolo `AWSServiceRoleForAmazonGuardDuty`, il ruolo collegato ai servizi `guardduty.amazonaws.com` considera attendibile il servizio.

Le politiche di autorizzazione aiutano a GuardDuty svolgere le seguenti attività:

- Usa le azioni di Amazon EC2 per gestire e recuperare informazioni sulle tue istanze EC2, immagini e componenti di rete come VPCs sottoreti e gateway di transito.
- Usa AWS Systems Manager le azioni per gestire le associazioni SSM sulle istanze Amazon EC2 quando GuardDuty abiliti il monitoraggio del runtime con agente automatizzato per Amazon EC2. Quando la configurazione GuardDuty automatizzata degli agenti è disabilitata, GuardDuty considera solo le istanze EC2 che hanno un tag di inclusione (:). GuardDutyManaged true
- Utilizza AWS Organizations le azioni per descrivere gli account e l'ID dell'organizzazione associati.
- Utilizzare le operazioni di Amazon S3 per recuperare informazioni su bucket e oggetti S3.
- Usa AWS Lambda le azioni per recuperare informazioni sulle funzioni e sui tag Lambda.
- Utilizzare le operazioni di Amazon EKS per gestire e recuperare informazioni sui cluster EKS e gestire i [Componenti aggiuntivi di Amazon EKS](#) su questi cluster. Le azioni EKS recuperano anche le informazioni sui tag associati a GuardDuty
- Usa IAM per creare il Malware Protection for EC2 [Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2](#) dopo che è stata abilitata.
- Utilizza le azioni Amazon ECS per gestire e recuperare informazioni sui cluster Amazon ECS e gestisci le impostazioni dell'account Amazon ECS con. guarddutyActivate Le azioni relative ad Amazon ECS recuperano anche le informazioni sui tag associati a GuardDuty

Il ruolo è configurato con le seguenti [policy gestite da AWS](#), denominate AmazonGuardDutyServiceRolePolicy.

Per esaminare le autorizzazioni relative a questa politica, consulta la AWS Managed Policy [AmazonGuardDutyServiceRolePolicy](#) Reference Guide.

Di seguito è riportata la policy di attendibilità associata al ruolo collegato ai servizi AWSServiceRoleForAmazonGuardDuty:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
```

```
    "Action": "sts:AssumeRole"
  }
]
}
```

Per i dettagli sugli aggiornamenti della AmazonGuardDutyServiceRolePolicy politica, consulta [GuardDuty aggiornamenti alle politiche gestite AWS](#). Per ricevere avvisi automatici sulle modifiche a questa politica, iscriviti al feed RSS presente nella [Cronologia dei documenti](#) pagina.

Creazione di un ruolo collegato al servizio per GuardDuty

Il ruolo AWSServiceRoleForAmazonGuardDuty collegato al servizio viene creato automaticamente quando lo si abilita GuardDuty per la prima volta o si abilita GuardDuty in una regione supportata in cui in precedenza non era abilitato. Puoi anche creare il ruolo collegato al servizio manualmente utilizzando la console IAM, l'API AWS CLI IAM.

Important

Il ruolo collegato al servizio creato per l'account amministratore GuardDuty delegato non si applica agli account dei membri. GuardDuty

Per consentire a un principale IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. AWSServiceRoleForAmazonGuardDuty Affinché il ruolo collegato al servizio venga creato correttamente, il principale IAM con cui lo utilizzi deve disporre delle autorizzazioni GuardDuty richieste. Per concedere le autorizzazioni richieste, collega la seguente policy gestita a questo utente, gruppo o ruolo .

Note

Sostituisci l'esempio riportato *account ID* nell'esempio seguente con il tuo ID effettivo.
Account AWS

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/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  }
]
}

```

Per ulteriori informazioni sulla creazione manuale del ruolo, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Modifica di un ruolo collegato al servizio per GuardDuty

GuardDuty non consente di modificare il ruolo collegato al AWSServiceRoleForAmazonGuardDuty servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile

tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per GuardDuty

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

Important

Se hai abilitato Malware Protection for EC2, l'eliminazione non comporta l'eliminazione automatica di `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Se desideri eliminare `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulta [Eliminazione di un ruolo collegato al servizio per Malware Protection for EC2](#).

Devi prima disabilitarlo GuardDuty in tutte le regioni in cui è abilitato per eliminare il `AWSServiceRoleForAmazonGuardDuty`. Se il GuardDuty servizio non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione non riesce. Per ulteriori informazioni, consulta [Sospensione o disabilitazione GuardDuty](#).

Quando si disattiva GuardDuty, `AWSServiceRoleForAmazonGuardDuty` non viene eliminato automaticamente. Se lo abiliti GuardDuty nuovamente, inizierà a utilizzare l'esistente `AWSServiceRoleForAmazonGuardDuty`.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l'API IAM per eliminare il ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Supportato Regioni AWS

Amazon GuardDuty supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio Regioni AWS ovunque GuardDuty sia disponibile. Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta gli [GuardDuty endpoint e le quote di Amazon](#) nel. Riferimenti generali di Amazon Web Services

Autorizzazioni di ruolo collegate ai servizi per Malware Protection for EC2

Malware Protection for EC2 utilizza il ruolo collegato al servizio (SLR) denominato.

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` Questa reflex consente a Malware Protection for EC2 di eseguire scansioni senza agenti per rilevare malware nel tuo account. GuardDuty Consente di GuardDuty creare un'istantanea del volume EBS nel tuo account e condividerla con l'account del servizio. GuardDuty Dopo aver GuardDuty valutato l'istantanea, include i metadati del carico di lavoro dell'istanza EC2 e del contenitore recuperati nei risultati di Malware Protection for EC2. Ai fini dell'assunzione del ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, il ruolo collegato ai servizi `malware-protection.guardduty.amazonaws.com` considera attendibile il servizio.

Le politiche di autorizzazione per questo ruolo aiutano Malware Protection for EC2 a svolgere le seguenti attività:

- Usa le azioni di Amazon Elastic Compute Cloud (Amazon EC2) per recuperare informazioni sulle istanze, i volumi e le istantanee di Amazon EC2. Malware Protection for EC2 fornisce anche l'autorizzazione per accedere ai metadati dei cluster Amazon EKS e Amazon ECS.
- Crea snapshot per volumi EBS con il tag `GuardDutyExcluded` non impostato su `true`. Per impostazione predefinita, gli snapshot vengono creati con un tag `GuardDutyScanId`. Non rimuovere questo tag, altrimenti Malware Protection for EC2 non avrà accesso alle istantanee.

Important

Se lo `GuardDutyExcluded` imposti su `true`, il GuardDuty servizio non sarà in grado di accedere a queste istantanee in futuro. Questo perché le altre istruzioni di questo ruolo collegato al servizio GuardDuty impediscono di eseguire qualsiasi azione sulle istantanee impostate su `GuardDutyExcluded true`

- Consenti la condivisione e l'eliminazione degli snapshot solo se il tag `GuardDutyScanId` esiste e se il tag `GuardDutyExcluded` non è impostato su `true`.

Note

Non consente a Malware Protection for EC2 di rendere pubbliche le istantanee.

- Accedi alle chiavi gestite dal cliente, ad eccezione di quelle con un `GuardDutyExcluded` tag impostato su `true`, da chiamare per creare e accedere `CreateGrant` a un volume EBS

crittografato dall'istantanea crittografata che viene condivisa con l'account del servizio. GuardDuty Per un elenco degli account di GuardDuty servizio per ogni regione, consulta. [GuardDuty account di servizio di Regione AWS](#)

- Accedi ai CloudWatch log dei clienti per creare il gruppo di log Malware Protection for EC2 e inserire i registri degli eventi di scansione del malware nel gruppo di log. `/aws/guardduty/malware-scan-events`
- Consenti al cliente di decidere se conservare nel proprio account gli snapshot su cui è stato rilevato il malware. Se la scansione rileva malware, il ruolo collegato al servizio consente di aggiungere due tag GuardDuty alle istantanee: `e. GuardDutyFindingDetected` `GuardDutyExcluded`

 Note

Il tag `GuardDutyFindingDetected` specifica che gli snapshot contengono malware.

- Determina se un volume è crittografato con una chiave gestita da EBS. GuardDuty esegue l'azione `DescribeKey` per determinare la key Id chiave gestita da EBS nel tuo account.
- Recupera l'istantanea dei volumi EBS crittografati utilizzando Chiave gestita da AWS, dal tuo Account AWS e copiala su. [GuardDuty account di servizio](#) A tal fine, utilizziamo le autorizzazioni `e. GetSnapshotBlock` `ListSnapshotBlocks` GuardDuty eseguirà quindi la scansione dell'istantanea nell'account del servizio. Attualmente, il supporto Malware Protection for EC2 per la scansione di volumi EBS crittografati con Chiave gestita da AWS potrebbe non essere disponibile in tutti i. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità di funzionalità specifiche per ogni regione](#).
- Consenti ad Amazon EC2 di effettuare chiamate per AWS KMS conto di Malware Protection for EC2 per eseguire diverse azioni crittografiche sulle chiavi gestite dal cliente. Operazioni come `kms:ReEncryptTo` e `kms:ReEncryptFrom` sono necessarie per condividere gli snapshot crittografati con le chiavi gestite dal cliente. Sono accessibili solo le chiavi per le quali il tag `GuardDutyExcluded` non è impostato su `true`.

Il ruolo è configurato con le seguenti [policy gestite da AWS](#), denominate `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Per esaminare le autorizzazioni relative a questa policy, consulta la AWS Managed Policy [AmazonGuardDutyMalwareProtectionServiceRolePolicy](#) Reference Guide.

La policy di attendibilità seguente è associata al ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creazione di un ruolo collegato al servizio per Malware Protection for EC2

Il ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio viene creato automaticamente quando abiliti Malware Protection for EC2 per la prima volta o abiliti Malware Protection for EC2 in una regione supportata in cui in precedenza non era abilitato. Puoi anche creare il ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente, utilizzando la console IAM, la CLI IAM o l'API IAM.

Note

Per impostazione predefinita, se sei un nuovo utente di Amazon GuardDuty, Malware Protection for EC2 è abilitato automaticamente.

Important

Il ruolo collegato al servizio creato per l'account GuardDuty amministratore delegato non si applica agli account dei membri. GuardDuty

Per consentire a un principale IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Affinché il ruolo collegato al

servizio venga creato correttamente, l'identità IAM con cui utilizzi deve disporre delle autorizzazioni GuardDuty richieste. Per concedere le autorizzazioni richieste, collega la seguente policy gestita a questo utente, gruppo o ruolo .

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"  
  }  
]  
}
```

Per ulteriori informazioni sulla creazione manuale del ruolo, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Modifica di un ruolo collegato al servizio per Malware Protection for EC2

Malware Protection for EC2 non consente di modificare il ruolo collegato al servizio.

AWSServiceRoleForAmazonGuardDutyMalwareProtection Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Malware Protection for EC2

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

Important

Per eliminare il **AWSServiceRoleForAmazonGuardDutyMalwareProtection**, devi prima disabilitare Malware Protection for EC2 in tutte le regioni in cui è abilitato.

Se Malware Protection for EC2 non è disabilitato quando tenti di eliminare il ruolo collegato al servizio, l'eliminazione avrà esito negativo. Assicurati di disabilitare innanzitutto Malware Protection for EC2 nel tuo account.

Quando scegli Disattiva per interrompere il servizio Malware Protection for EC2, non **AWSServiceRoleForAmazonGuardDutyMalwareProtection** viene eliminato automaticamente. Se poi scegli Abilita per avviare nuovamente il servizio Malware Protection for EC2, GuardDuty inizierà a utilizzare il servizio esistente.

AWSServiceRoleForAmazonGuardDutyMalwareProtection

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la AWS CLI o l'API IAM per eliminare il ruolo collegato al `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Supportato Regioni AWS

Amazon GuardDuty supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio in tutti i paesi in Regioni AWS cui è disponibile Malware Protection for EC2.

Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta gli [GuardDuty endpoint e le quote di Amazon](#) nel. Riferimenti generali di Amazon Web Services

Note

Malware Protection for EC2 non è attualmente disponibile negli AWS GovCloud Stati Uniti orientali e AWS GovCloud negli Stati Uniti occidentali.

AWS politiche gestite per Amazon GuardDuty

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. La [creazione di policy gestite dai clienti IAM](#) che forniscono al team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nell'account Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le [policy AWS gestite](#) nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ReadOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni

di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consultare la sezione [Policy gestite da AWS per funzioni di processi](#) nella Guida per l'utente di IAM.

L'elemento della policy `Version` specifica le regole sintattiche di linguaggio che devono essere utilizzate per elaborare una policy. Le seguenti politiche includono la versione corrente supportata da IAM. Per ulteriori informazioni, consulta [IAM JSON Policy elements: Version](#).

AWS politica gestita: AmazonGuardDutyFullAccess_v2 (consigliata)

È possibile allegare la policy `AmazonGuardDutyFullAccess_v2` alle identità IAM. Questa politica consentirà a un utente l'accesso completo per eseguire tutte le GuardDuty azioni e accedere alle risorse richieste. Between `AmazonGuardDutyFullAccess_v2` and `AmazonGuardDutyFullAccess`, GuardDuty consiglia il collegamento `AmazonGuardDutyFullAccess_v2` perché offre una maggiore sicurezza e limita le azioni amministrative ai responsabili del GuardDuty servizio.

Dettagli dell'autorizzazione

La `AmazonGuardDutyFullAccess_v2` politica include le seguenti autorizzazioni:

- GuardDuty— Consente agli utenti l'accesso completo a tutte le GuardDuty azioni.
- IAM:
 - Consente agli utenti di creare ruoli GuardDuty collegati al servizio.
 - Consente di visualizzare e gestire i ruoli IAM e le relative politiche per GuardDuty
 - Consente agli utenti di passare un ruolo a GuardDuty. GuardDuty utilizza questo ruolo per abilitare Malware Protection for S3 e scansionare gli oggetti S3 alla ricerca di malware. GuardDuty utilizza questo ruolo anche per avviare scansioni per Malware Protection for Backup AWS .
 - L'autorizzazione a eseguire un'iam:GetRoleazione `AWSServiceRoleForAmazonGuardDutyMalwareProtection` stabilisce se il ruolo collegato al servizio (SLR) per Malware Protection for EC2 esiste in un account.
- Organizations:
 - Consenti agli utenti di leggere (visualizzare) GuardDuty la struttura organizzativa e gli account.
 - Consente agli utenti di designare un amministratore delegato e gestire i membri di un' GuardDuty organizzazione.

Per esaminare le autorizzazioni per questa politica, vedere [AmazonGuardDutyFullAccess_v2](#) nella Managed Policy Reference Guide.AWS

AWS politica gestita: AmazonGuardDutyFullAccess

È possibile allegare la policy AmazonGuardDutyFullAccess alle identità IAM.

Important

Per una maggiore sicurezza e autorizzazioni restrittive ai responsabili GuardDuty del servizio, ti consigliamo di utilizzare. [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#)

Questa politica concede autorizzazioni amministrative che consentono a un utente l'accesso completo per eseguire tutte le azioni e le risorse. GuardDuty

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- **GuardDuty**— Consente agli utenti l'accesso completo a tutte le GuardDuty azioni.
- **IAM**:
 - Consente agli utenti di creare il ruolo GuardDuty collegato al servizio.
 - Consente a un account amministratore di abilitare gli account GuardDuty dei membri.
 - Consente agli utenti di passare un ruolo a GuardDuty. GuardDuty utilizza questo ruolo per abilitare Malware Protection for S3 e scansione degli oggetti S3 alla ricerca di malware. GuardDuty utilizza questo ruolo anche per avviare scansioni per Malware Protection for Backup AWS .
- **Organizations**— Consente agli utenti di designare un amministratore delegato e gestire i membri di un'organizzazione. GuardDuty

L'autorizzazione a eseguire un'iam:GetRoleazione

AWSServiceRoleForAmazonGuardDutyMalwareProtection stabilisce se il ruolo collegato al servizio (SLR) per Malware Protection for EC2 esiste in un account.

Per esaminare le autorizzazioni relative a questa policy, consulta la Managed Policy Reference [AmazonGuardDutyFullAccess](#)Guide.AWS

AWS politica gestita: AmazonGuardDutyReadOnlyAccess

È possibile allegare la policy AmazonGuardDutyReadOnlyAccess alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono a un utente di visualizzare GuardDuty i risultati e i dettagli dell'organizzazione. GuardDuty

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **GuardDuty**— Consente agli utenti di visualizzare GuardDuty i risultati ed eseguire operazioni API che iniziano con `Get`, o. `List Describe`
- **Organizations**— Consente agli utenti di recuperare informazioni sulla configurazione GuardDuty dell'organizzazione, inclusi i dettagli dell'account amministratore delegato.

Per esaminare le autorizzazioni relative a questa politica, consulta [AmazonGuardDutyReadOnlyAccess](#)la AWS Managed Policy Reference Guide.

AWS politica gestita: AmazonGuardDutyServiceRolePolicy

Non è possibile collegare AmazonGuardDutyServiceRolePolicy alle entità IAM. Questa policy AWS gestita è associata a un ruolo collegato al servizio che consente di eseguire azioni GuardDuty per conto dell'utente. Per ulteriori informazioni, consulta [Autorizzazioni di ruolo collegate al servizio per GuardDuty](#).

GuardDuty aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite GuardDuty da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei GuardDuty documenti.

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy : aggiornamento a una policy esistente	È stata aggiunta l'cloudtrail:CreateServiceLinkedChannel autorizzazione per abilitare un meccanismo aggiuntivo per la AWS CloudTrail fruizione degli eventi. <pre> { "Sid": "CloudTrailCreateServiceLinkedChannelSid", "Effect": "Allow", "Action": ["cloudtrail:CreateServiceLinkedChannel"], "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*", "Condition": { "StringEquals": { "aws:ResourceAccount": </pre>	25 marzo 2026

Modifica	Descrizione	Data
	<pre>nt": "\${aws:PrincipalAccount}" } } }</pre>	
AmazonGuardDutyFullAccess : obsoleta	Questa policy è stata sostituita da una policy ad ambito ridotto denominata AmazonGuardDutyFullAccess_v2 . Dopo il 13 marzo 2026, non puoi allegare la AmazonGuardDutyFullAccess politica a nuovi utenti, gruppi o ruoli. Per ulteriori informazioni, consulta AWS politica gestita: AmazonGuardDutyFullAccess_v2 (consigliata).	13 marzo 2026

Modifica	Descrizione	Data
AmazonGuardDutyFullAccess_v2 : aggiornamento di una policy esistente	È stata aggiunta l'autorizzazione che consente di passare un ruolo IAM a GuardDuty quando si attiva Malware Protection for AWS Backup. <pre>{ "Sid": "AllowPassRoleToMalwareProtection", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": ["malware-protectio"</pre>	19 novembre 2025

Modifica	Descrizione	Data
	<pre>n-plan.guardduty.a mazonaws.com", "malware-protectio n.guardduty.amazon aws.com"] } } }</pre>	

Modifica	Descrizione	Data
AmazonGuardDutyFullAccess : aggiornamento di una policy esistente	È stata aggiunta l'autorizzazione che consente di passare un ruolo IAM a GuardDuty quando si attiva Malware Protection for AWS Backup. <pre>{ "Sid": "AllowPassRoleToMa lwareProtection", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/ *", "Conditio n": { "StringEquals": { "iam:PassedToServi ce": ["malware-protectio</pre>	19 novembre 2025

Modifica	Descrizione	Data
	<pre>n-plan.guardduty.a mazonaws.com", "malware-protectio n.guardduty.amazon aws.com"] } } }</pre>	
AmazonGuardDutyFullAccess_v2 — Aggiunta una nuova politica	Aggiunta una nuova AmazonGuardDutyFullAccess_v2 politica. Questa opzione è consigliata perché le relative autorizzazioni migliorano la sicurezza limitando le azioni amministrative ai responsabili dei GuardDuty servizi in base ai ruoli e alle policy di IAM e all'integrazione. AWS Organizations	4 giugno 2025
AmazonGuardDutyServiceRolePolicy : aggiornamento di una policy esistente	È stata aggiunta l'ec2:DescribeVpcs autorizzazione. Ciò consente di GuardDuty tenere traccia degli aggiornamenti del VPC, ad esempio il recupero del VPC CIDR.	22 agosto 2024

Modifica	Descrizione	Data
AmazonGuardDutyFullAccess : aggiornamento di una policy esistente	È stata aggiunta un'autorizzazione che consente di assegnare un ruolo IAM a GuardDuty quando si attiva Malware Protection for S3. <pre>{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com" } } }</pre>	10 giugno 2024

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy : aggiorna a una policy esistente.	Usa AWS Systems Manager le azioni per gestire le associazioni SSM sulle istanze Amazon EC2 quando GuardDuty abilita il monitoraggio del runtime con agente automatizzato per Amazon EC2. Quando la configurazione GuardDuty automatizzata degli agenti è disabilitata, GuardDuty considera solo le istanze EC2 che hanno un tag di inclusione (:). GuardDuty Managed true	26 marzo 2024
AmazonGuardDutyServiceRolePolicy : aggiorna a una policy esistente.	GuardDuty ha aggiunto una nuova autorizzazione: <code>organization:DescribeOrganization</code> recuperare l'ID dell'organizzazione dell'account Amazon VPC condiviso e impostare la policy degli endpoint Amazon VPC con l'ID dell'organizzazione.	9 febbraio 2024

Modifica	Descrizione	Data
AmazonGuardDutyMalwareProtectionServiceRolePolicy : aggiorna a una policy esistente.	Malware Protection for EC2 ha aggiunto due autorizzazioni: GetSnapshotBlock quella di ListSnapshotBlocks recuperare l'istantanea di un volume EBS (con crittografia Chiave gestita da AWS) dall'utente Account AWS e copiarla nell'account del GuardDuty servizio prima di avviare la scansione antimalware.	25 gennaio 2024
AmazonGuardDutyServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte nuove autorizzazioni per consentire di GuardDuty aggiungere e l'impostazione dell'account guarddutyActivate Amazon ECS ed eseguire operazioni, elencare e descrivere sui cluster Amazon ECS.	26 novembre 2023
AmazonGuardDutyReadOnlyAccess : aggiornamento di una policy esistente	GuardDuty ha aggiunto una nuova politica organizations per. ListAccounts	16 novembre 2023
AmazonGuardDutyFullAccess : aggiornamento di una policy esistente	GuardDuty ha aggiunto una nuova politica organizations perListAccounts .	16 novembre 2023

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy : aggiornamento di una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per supportare la prossima funzionalità GuardDuty EKS Runtime Monitoring.	8 marzo 2023
AmazonGuardDutyServiceRolePolicy : aggiornamento di una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per consentire la creazione di un ruolo collegato GuardDuty al servizio per Malware Protection for EC2. Ciò contribuirà a GuardDuty semplificare il processo di attivazione di Malware Protection for EC2. GuardDuty ora può eseguire la seguente azione IAM: <pre>{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }</pre>	21 febbraio 2023

Modifica	Descrizione	Data
AmazonGuardDutyFullAccess: aggiornamento di una policy esistente	GuardDuty ARN aggiornato per <code>iam:GetRole</code> to. <code>*AWSServiceRoleForAmazonGuardDutyMalwareProtection</code>	26 luglio 2022
AmazonGuardDutyFullAccess: aggiornamento di una policy esistente	GuardDuty ha aggiunto un nuovo <code>AWSServiceName</code> per consentire la creazione di ruoli collegati al servizio utilizzando il servizio GuardDuty Malware Protection <code>iam:CreateServiceLinkedRole</code> for EC2. GuardDuty ora può eseguire l'<code>iam:GetRole</code> azione per ottenere informazioni per <code>AWSServiceRole</code>	26 luglio 2022

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy : aggiornamento di una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per consentire di GuardDuty utilizzare le azioni di rete di Amazon EC2 per migliorare i risultati. GuardDuty ora puoi eseguire le seguenti azioni EC2 per ottenere informazioni su come comunicano le tue istanze EC2. Queste informazioni vengono utilizzate per migliorare la precisione degli esiti. • <code>ec2:DescribeVpcEndpoints</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:DescribeVpcPeeringConnections</code> • <code>ec2:DescribeTransitGatewayAttachments</code>	3 agosto 2021
GuardDuty ha iniziato a tenere traccia delle modifiche	GuardDuty ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	3 agosto 2021

Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con GuardDuty e IAM.

Argomenti

- [Non sono autorizzato a eseguire alcuna azione in GuardDuty](#)
- [Non sono autorizzato a eseguire iam:PassRole.](#)
- [Voglio consentire a persone esterne Account AWS a me di accedere alle mie GuardDuty risorse.](#)

Non sono autorizzato a eseguire alcuna azione in GuardDuty

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni guardduty: `GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
guardduty:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione guardduty: `GetWidget`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole.

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a GuardDuty.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in GuardDuty. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne Account AWS a me di accedere alle mie GuardDuty risorse.

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se GuardDuty supporta queste funzionalità, consulta [Come GuardDuty funziona Amazon con IAM](#)
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Convalida della conformità per Amazon GuardDuty

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la [Documentazione AWS sulla sicurezza](#).

Resilienza in Amazon GuardDuty

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta [infrastruttura AWS globale](#).

Sicurezza dell'infrastruttura in Amazon GuardDuty

In quanto servizio gestito, Amazon GuardDuty è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere GuardDuty attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Amazon GuardDuty e gli endpoint VPC di interfaccia ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e Amazon GuardDuty creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono alimentati da [AWS PrivateLink](#), una tecnologia

che consente l'accesso privato GuardDuty APIs senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione AWS Direct Connect. Le istanze del tuo VPC non necessitano di indirizzi IP pubblici con cui comunicare. GuardDuty APIs Il traffico tra il tuo VPC e GuardDuty non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più [interfacce di rete elastiche](#) nelle sottoreti.

Per ulteriori informazioni, consulta [Interface VPC endpoints \(AWS PrivateLink\) nella Guida](#).AWS PrivateLink

Considerazioni sugli endpoint GuardDuty VPC

Prima di configurare un endpoint VPC di interfaccia per GuardDuty, assicurati di esaminare le [proprietà e le limitazioni dell'endpoint dell'interfaccia](#) nella Guida.AWS PrivateLink

GuardDuty supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC.

Creazione di un endpoint VPC di interfaccia per GuardDuty

Puoi creare un endpoint VPC per il GuardDuty servizio utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint VPC per GuardDuty utilizzare il seguente nome di servizio:

- com.amazonaws. *region*.servizio di guardia
- com.amazonaws.it. *region*.guardduty-fips (endpoint FIPS)

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API GuardDuty utilizzando il nome DNS predefinito per la regione, ad esempio. guardduty.us-east-1.amazonaws.com

Per ulteriori informazioni, consulta [Accedere a un servizio tramite un endpoint di interfaccia](#) nella Guida.AWS PrivateLink

Creazione di una policy per gli endpoint VPC per GuardDuty

È possibile allegare un criterio all'endpoint VPC che controlla l'accesso all' GuardDuty. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni, consulta [Controllare l'accesso ai servizi con endpoint VPC nella Guida AWS PrivateLink](#)

Esempio: policy degli endpoint VPC per le azioni GuardDuty

Di seguito è riportato un esempio di policy sugli endpoint per GuardDuty. Se associata a un endpoint, questa politica consente l'accesso alle GuardDuty azioni elencate per tutti i principali su tutte le risorse.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "guardduty:listDetectors",
        "guardduty:getDetector",
        "guardduty:getFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Sottoreti condivise

Non puoi creare, descrivere, modificare o eliminare gli endpoint VPC nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli endpoint VPC in sottoreti condivise con te. Per informazioni sulla condivisione VPC, consulta la pagina [Condivisione del VPC con altri account](#) nella Guida per l'utente di Amazon VPC.

GuardDuty integrazione con i servizi AWS di sicurezza

GuardDuty può essere integrato con altri servizi AWS di sicurezza. Questi servizi possono GuardDuty importare dati da cui visualizzare i risultati in modi nuovi. Consulta le seguenti opzioni di integrazione per saperne di più su come il servizio è configurato per funzionare. GuardDuty

Integrazione con GuardDuty AWS Security Hub CSPM

AWS Security Hub CSPM raccoglie dati di sicurezza da tutti AWS gli account, i servizi e i prodotti partner di terze parti supportati per valutare lo stato di sicurezza dell'ambiente in base agli standard e alle migliori pratiche del settore. Oltre a valutare il livello di sicurezza, Security Hub CSPM crea una posizione centrale per i risultati di tutti i AWS servizi integrati e i prodotti dei partner. AWS L'attivazione di Security Hub CSPM con GuardDuty consentirà automaticamente l'acquisizione dei dati dei GuardDuty risultati da parte di Security Hub CSPM.

Per ulteriori informazioni sull'utilizzo di Security Hub CSPM, vedere. GuardDuty [Integrazione con AWS Security Hub CSPM](#)

Integrazione GuardDuty con Amazon Detective

Amazon Detective utilizza i dati di log di tutti AWS i tuoi account per creare visualizzazioni di dati per le tue risorse e gli indirizzi IP che interagiscono con il tuo ambiente. Le visualizzazioni di Detective sono utili per indagare in modo rapido e semplice sui problemi di sicurezza. Puoi passare dalla GuardDuty ricerca dei dettagli alle informazioni nella console Detective una volta abilitati entrambi i servizi.

Per ulteriori informazioni sull'utilizzo di Detective, GuardDuty vedere [Integrazione con Amazon Detective](#).

Integrazione con AWS Security Hub CSPM

[AWS Security Hub CSPM](#) fornisce una visione completa dello stato di sicurezza in AWS e ti aiuta a controllare l'ambiente rispetto agli standard di sicurezza del settore e alle best practice. Security Hub CSPM raccoglie dati sulla sicurezza da AWS account, servizi e prodotti partner di terze parti supportati e ti aiuta ad analizzare le tendenze della sicurezza e identificare i problemi di sicurezza con la massima priorità.

L' GuardDuty integrazione di Amazon con Security Hub CSPM ti consente di inviare i risultati da GuardDuty Security Hub CSPM. Security Hub CSPM può quindi includere tali risultati nell'analisi del livello di sicurezza dell'utente.

Indice

- [In che modo Amazon GuardDuty invia i risultati a AWS Security Hub CSPM](#)
 - [Tipi di risultati che vengono GuardDuty inviati a Security Hub CSPM](#)
 - [Latenza per l'invio di nuovi risultati](#)
 - [Riprovare quando Security Hub CSPM non è disponibile](#)
 - [Aggiornamento degli esiti esistenti CSPM Security Hub](#)
- [Visualizzazione dei GuardDuty risultati in AWS Security Hub CSPM](#)
 - [Interpretazione dei nomi GuardDuty dei risultati in AWS Security Hub CSPM](#)
 - [Risultato tipico di GuardDuty](#)
- [Abilitazione e configurazione dell'integrazione](#)
- [Utilizzo GuardDuty dei controlli in Security Hub CSPM](#)
- [Interruzione della pubblicazione dei risultati su Security Hub CSPM](#)

In che modo Amazon GuardDuty invia i risultati a AWS Security Hub CSPM

Nel AWS Security Hub CSPM, i problemi di sicurezza vengono registrati come risultati. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub CSPM dispone anche di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

CSPM Security Hub fornisce strumenti per gestire gli esiti da tutte queste origini. È possibile visualizzare e filtrare gli elenchi di esiti e visualizzare i dettagli per un riscontro. Per ulteriori informazioni, consulta [Visualizzazione degli esiti](#) nella Guida per l'utente AWS Security Hub . È inoltre possibile monitorare lo stato di un'indagine in un esito. Per ulteriori informazioni, consulta [Operazioni sugli esiti](#) nella Guida per l'utente di AWS Security Hub .

Tutti i risultati in Security Hub CSPM utilizzano un formato JSON standard chiamato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato corrente dell'esito. Consulta [AWS Security Finding Format \(ASFF\)](#) nella Guida per l'utente di AWS Security Hub .

Amazon GuardDuty è uno dei AWS servizi che invia i risultati al Security Hub CSPM.

Tipi di risultati che vengono GuardDuty inviati a Security Hub CSPM

Una volta abilitato GuardDuty Security Hub CSPM nello stesso account all'interno dello stesso Regione AWS, GuardDuty inizia a inviare tutti i risultati generati a Security Hub CSPM. Questi risultati vengono inviati a Security Hub CSPM utilizzando il [AWS Security Finding Format \(ASFF\)](#). In ASFF, il Types campo fornisce il tipo di esito.

Latenza per l'invio di nuovi risultati

Quando viene GuardDuty creato un nuovo risultato, di solito viene inviato a Security Hub CSPM entro cinque minuti.

Riprovare quando Security Hub CSPM non è disponibile

Se Security Hub CSPM non è disponibile, GuardDuty riprova a inviare i risultati finché non vengono ricevuti.

Aggiornamento degli esiti esistenti CSPM Security Hub

Dopo aver inviato un risultato a Security Hub CSPM, GuardDuty invia aggiornamenti per riflettere ulteriori osservazioni sull'attività di ricerca a Security Hub CSPM. Le nuove osservazioni di questi risultati vengono inviate a Security Hub CSPM in base alle [Fase 5 — Frequenza di esportazione dei risultati](#) impostazioni del tuo. Account AWS

Quando archivi o annulli l'archiviazione di un risultato, GuardDuty non lo invia a Security Hub CSPM. Qualsiasi risultato non archiviato manualmente e che successivamente diventerà attivo in non GuardDuty viene inviato a Security Hub CSPM.

Visualizzazione dei GuardDuty risultati in AWS Security Hub CSPM

Accedi a Console di gestione AWS e apri la AWS Security Hub CSPM console all'indirizzo <https://console.aws.amazon.com/securityhub/>.

È ora possibile utilizzare uno dei seguenti modi per visualizzare i GuardDuty risultati nella console CSPM di Security Hub:

Opzione 1: utilizzo delle integrazioni in Security Hub CSPM

1. Nel riquadro di navigazione a sinistra, scegli Integrazioni.
2. Nella pagina Integrazioni, controlla lo stato di Amazon: GuardDuty.

- Se lo stato è Accettazione dei risultati, quindi scegli Vedi risultati accanto a Accettazione dei risultati.
- In caso contrario, per ulteriori informazioni su come funzionano le integrazioni, consulta le integrazioni [CSPM di Security Hub](#) nella Guida per l'utente AWS Security Hub

Opzione 2: utilizzo dei risultati in Security Hub CSPM

1. Nel riquadro di navigazione a sinistra, scegli Findings.
2. Nella pagina Risultati, aggiungi il filtro Nome prodotto e inserisci **GuardDuty** per visualizzare solo GuardDuty i risultati.

Interpretazione dei nomi GuardDuty dei risultati in AWS Security Hub CSPM

GuardDuty invia i risultati a Security Hub CSPM utilizzando il [AWS Security Finding Format \(ASFF\)](#). In ASFF, il Types campo fornisce il tipo di esito. I tipi ASFF utilizzano uno schema di denominazione diverso rispetto ai tipi GuardDuty. La tabella seguente descrive in dettaglio tutti i tipi GuardDuty di risultati con la loro controparte ASFF così come appaiono in Security Hub CSPM.

Note

Per alcuni tipi di GuardDuty ricerca, Security Hub CSPM assegna nomi di ricerca ASFF diversi a seconda che il ruolo della risorsa del dettaglio del risultato sia ACTOR o TARGET. Per ulteriori informazioni, consulta [Dettagli degli esiti](#).

GuardDuty tipo di ricerca	Tipo di risultati ASFF
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedC redentials
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/KernelModuleLoaded	TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded
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
Scoperta: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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
Execution:S3/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:S3-MaliciousFile!RecoveryPoint
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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
Persistenza:/IAMUserAnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
PrivilegeEscalation:Runtime/SuspiciousCommand	Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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.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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
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

Risultato tipico di GuardDuty

GuardDuty invia i risultati al Security Hub CSPM utilizzando il [AWS Security Finding Format \(ASFF\)](#).

Ecco un esempio di un risultato tipico di 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"  
}
```

Abilitazione e configurazione dell'integrazione

Per utilizzare l'integrazione con AWS Security Hub CSPM, è necessario abilitare Security Hub CSPM. Per informazioni su come abilitare Security Hub CSPM, vedere [Configurazione di Security Hub nella Guida](#) per l'AWS Security Hub utente.

Quando abiliti entrambi GuardDuty e Security Hub CSPM, l'integrazione viene abilitata automaticamente. GuardDuty inizia immediatamente a inviare i risultati al Security Hub CSPM.

Utilizzo GuardDuty dei controlli in Security Hub CSPM

AWS Security Hub CSPM utilizza i controlli di sicurezza per valutare le AWS risorse e verificare la conformità rispetto agli standard e alle best practice del settore della sicurezza. È possibile utilizzare i controlli relativi alle GuardDuty risorse e ai piani di protezione selezionati. Per ulteriori informazioni, consulta [GuardDuty controlli di Amazon](#) nella Guida AWS Security Hub per l'utente.

Per un elenco di tutti i controlli tra AWS servizi e risorse, consulta il [riferimento ai controlli CSPM di Security Hub nella Guida](#) per l'AWS Security Hub utente.

Interruzione della pubblicazione dei risultati su Security Hub CSPM

Per interrompere l'invio degli esiti a CSPM Security Hub, è possibile utilizzare la console CSPM Security Hub o l'API.

Vedi [Disabilitazione e abilitazione del flusso di risultati da un'integrazione \(console\)](#) o [Disabilitazione del flusso di risultati da un'integrazione \(Security Hub API, AWS CLI\)](#) nella Guida per l'utente AWS Security Hub

Integrazione con Amazon Detective

[Amazon Detective](#) ti aiuta ad analizzare e indagare rapidamente sugli eventi di sicurezza su uno o più AWS account generando visualizzazioni di dati che rappresentano il modo in cui le tue risorse si comportano e interagiscono nel tempo. Detective crea visualizzazioni dei risultati. GuardDuty

Detective acquisisce i dettagli di tutti ogni tipo di esito e fornisce l'accesso ai profili delle entità per indagare su quelle coinvolte negli esiti. Un'entità può essere una Account AWS AWS risorsa

all'interno di un account o un indirizzo IP esterno che ha interagito con le tue risorse. La GuardDuty console supporta il passaggio ad Amazon Detective dalle seguenti entità, a seconda del tipo di risultato: ruolo IAM Account AWS, utente o sessione di ruolo, agente utente, utente federato, istanza Amazon EC2 o indirizzo IP.

Indice

- [Abilitazione dell'integrazione](#)
- [Passare ad Amazon Detective partendo da una scoperta GuardDuty](#)
- [Utilizzo dell'integrazione con un ambiente GuardDuty multi-account](#)

Abilitazione dell'integrazione

Per utilizzare Amazon Detective con GuardDuty, devi prima abilitare Amazon Detective. Per informazioni su come abilitare Detective, consulta la sezione Guida [introduttiva ad Amazon Detective](#) nella Amazon Detective User Guide.

Quando abiliti entrambi GuardDuty e Detective, l'integrazione viene abilitata automaticamente. Una volta abilitato, Detective acquisirà immediatamente i dati dei GuardDuty risultati.

Note

GuardDuty invia i risultati al Detective in base alla frequenza di esportazione dei GuardDuty risultati. Per impostazione predefinita, la frequenza di esportazione per gli aggiornamenti agli esiti esistenti è di 6 ore. Per garantire che Detective riceva gli aggiornamenti più recenti sulle tue scoperte, ti consigliamo di modificare la frequenza di esportazione a 15 minuti in ogni regione in cui utilizzi Detective GuardDuty. Per ulteriori informazioni, consulta [Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati](#).

Passare ad Amazon Detective partendo da una scoperta GuardDuty

1. Accedi alla console. <https://console.aws.amazon.com/guardduty/>
2. Scegli un singolo esito dalla tabella degli esiti.
3. Scegli Esamina con Detective dal riquadro dei dettagli dell'esito.
4. Scegli un aspetto dell'esito su cui indagare con Amazon Detective. Così facendo si apre la console Detective per l'esito o entità in questione.

Se il pivot non si comporta come previsto, consulta [Risoluzione dei problemi del pivot nella Guida per l'utente di Amazon Detective](#).

 Note

Se archivi un GuardDuty risultato nella console Detective, quel risultato viene archiviato anche nella GuardDuty console.

Utilizzo dell'integrazione con un ambiente GuardDuty multi-account

Se gestisci un ambiente con più account in GuardDuty, devi aggiungere i tuoi account membro ad Amazon Detective per visualizzare le visualizzazioni dei dati di Detective relativi ai risultati e alle entità presenti in tali account.

Si consiglia di utilizzare lo stesso account GuardDuty amministratore dell'account amministratore di Detective. Per ulteriori informazioni sull'aggiunta di account membro in Detective, consulta la sezione [Gestione degli account](#) nella Amazon Detective User Guide.

 Note

Detective è un servizio regionale, perciò devi abilitare Detective e aggiungere i tuoi account membri in ogni regione in cui desideri utilizzare l'integrazione.

Sospensione o disabilitazione GuardDuty

Puoi utilizzare la GuardDuty console per sospendere o disabilitare il servizio. GuardDuty Non ti viene addebitato alcun costo per l'utilizzo GuardDuty quando il servizio è sospeso.

- Tutti gli account dei membri devono essere dissociati o eliminati prima di poter sospendere o disabilitare. GuardDuty
- Se si sospende GuardDuty, la sospensione non monitora più la sicurezza dell' AWS ambiente né genera nuovi risultati. I risultati esistenti rimangono intatti e non sono influenzati dalla sospensione. GuardDuty Puoi scegliere di GuardDuty riattivarla in un secondo momento.
- La disattivazione GuardDuty in un account verrà disattivata solo per l'account attualmente selezionato Regione AWS. Se desideri disabilitarlo completamente GuardDuty, devi disabilitarlo in ogni regione in cui è abilitato.
- Se disabiliti GuardDuty, i risultati e la GuardDuty configurazione esistenti vengono persi e non possono essere recuperati. Se desideri salvare i risultati esistenti, devi esportarli prima di confermarne la disabilitazione GuardDuty. Per informazioni su come esportare gli esiti, consulta [Esportazione dei risultati generati su Amazon S3](#).
- Se hai abilitato Malware Protection for S3 per uno o più bucket protetti nel tuo account, la sospensione o la disabilitazione GuardDuty non influiscono sullo stato di un bucket protetto in Malware Protection for S3. Anche dopo la sospensione o la disattivazione GuardDuty, il tuo account continuerà a sostenere i costi di utilizzo associati alla funzionalità Malware Protection for S3. Per informazioni sulla disabilitazione di Malware Protection for S3, consulta. [Disattivazione di Malware Protection for S3 per un bucket protetto](#)

Per sospendere o disabilitare GuardDuty

1. Apri la GuardDuty console all'indirizzo <https://console.aws.amazon.com/guardduty/>.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella GuardDuty sezione Sospendi, scegli Sospendi GuardDuty o Disattiva GuardDuty, quindi Conferma l'azione.

Da riattivare dopo la sospensione GuardDuty

1. Apri la GuardDuty console all'indirizzo. <https://console.aws.amazon.com/guardduty/>
2. Nel pannello di navigazione scegli Impostazioni.

3. Scegli Riattiva GuardDuty

Iscrizione agli annunci di Amazon SNS GuardDuty

Questa sezione fornisce informazioni sulla sottoscrizione ad Amazon SNS (Simple Notification Service) GuardDuty per gli annunci di ricezione di notifiche sui tipi di risultati appena rilasciati, aggiornamenti ai tipi di risultati esistenti e altre modifiche alle funzionalità. Le notifiche sono disponibili in tutti i formati supportati da Amazon SNS.

Il GuardDuty SNS invia annunci sugli aggiornamenti del GuardDuty servizio a qualsiasi account sottoscritto. AWS Per ricevere notifiche sugli esiti all'interno del tuo account, consulta [Elaborazione dei GuardDuty risultati con Amazon EventBridge](#).

Note

Il tuo utente IAM deve disporre delle autorizzazioni `sns::subscribe` per sottoscrivere un argomento SNS.

Puoi sottoscrivere una coda Amazon SQS a questo argomento di notifica, ma devi utilizzare un ARN dell'argomento che si trovi nella stessa regione. Per ulteriori informazioni, consulta [Tutorial: sottoscrizione di una coda Amazon SQS a un argomento Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Queue Service.

Puoi anche utilizzare una AWS Lambda funzione per attivare eventi quando vengono ricevute notifiche. Per ulteriori informazioni, consulta [Richiamo delle funzioni Lambda tramite le notifiche di Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Queue Service.

Di seguito è riportato l'argomento Amazon SNS ARNs per ciascuna regione.

Regione AWS	ARN di un argomento Amazon SNS
Stati Uniti orientali (Virginia settentrionale) - us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements
Stati Uniti orientali (Ohio) - us-east-2	arn:aws:sns:us-east-2:118283430703:G

Regione AWS	ARN di un argomento Amazon SNS
	uardDutyAnnounceme nts
Stati Uniti occidentali (California settentrionale) - us-west-1	arn:aws:sns:us-wes t-1:144182107116:G uardDutyAnnounceme nts
Stati Uniti occidentali (Oregon) - us-west-2	arn:aws:sns:us-wes t-2:934957504740:G uardDutyAnnounceme nts
Canada (Centrale) - ca-central-1	arn:aws:sns:ca-cen tral-1:10743005193 3:GuardDutyAnnounc ements
Canada occidentale (Calgary) - ca-west-1	arn:aws:sns:ca-wes t-1:440427180217:G uardDutyAnnounceme nts
Europa (Stoccolma) - eu-north-1	arn:aws:sns:eu-nor th-1:973841112453: GuardDutyAnnouncem ents
Europa (Irlanda) - eu-west-1	arn:aws:sns:eu-wes t-1:965013871422:G uardDutyAnnounceme nts

Regione AWS	ARN di un argomento Amazon SNS
Europa (Londra) - eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
Europa (Parigi) - eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
Europa (Francoforte) - eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
Europa (Zurigo) - eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
Asia Pacifico (Hong Kong) - ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
Asia Pacifico (Tokyo) - ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
Asia Pacifico (Seoul) - ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

Regione AWS	ARN di un argomento Amazon SNS
Asia Pacifico (Singapore) - ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
Asia Pacifico (Sydney) - ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
Asia Pacifico (Mumbai) - ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
Sud America (San Paolo) - sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
AWS GovCloud (Stati Uniti occidentali) - us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
Cina (Pechino) - cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
Cina (Ningxia) - cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

Regione AWS	ARN di un argomento Amazon SNS
Medio Oriente (Bahrein) - me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
Medio Oriente (EAU) - me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
Europa (Milano) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Europa (Spagna) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (Stati Uniti orientali) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asia Pacifico (Osaka): ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Asia Pacifico (Giacarta) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

Regione AWS	ARN di un argomento Amazon SNS
Asia Pacifico (Hyderabad) - ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
Asia Pacifico (Melbourne) - ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
Asia Pacifico (Malesia) - ap-southeast-5	arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements
Israele (Tel Aviv) - il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements
Asia Pacifico (Tailandia) - ap-southeast-7	arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements
Messico (Centrale) - mx-central-1	arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements
Asia Pacifico (Taipei) - ap-east-2	arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements

Per iscriverti all'e-mail di notifica dell' GuardDuty aggiornamento nel Console di gestione AWS

1. [Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
2. Nell'elenco delle regioni, scegli la stessa regione dell'argomento ARN da sottoscrivere. Questo esempio utilizza la regione us-west-2.
3. Nel riquadro di navigazione a sinistra, scegli Subscriptions (Abbonamenti), quindi Create subscription (Crea abbonamento).
4. Nella finestra di dialogo Create Subscription (Crea sottoscrizione), in Topic ARN (ARN argomento), incolla l'ARN dell'argomento: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Per Protocollo, scegli E-mail. Per Endpoint, digitare l'indirizzo e-mail a cui deve essere inviata la notifica.
6. Scegli Create Subscription (Crea sottoscrizione).
7. Nella tua applicazione di posta elettronica, apri il messaggio da AWS Notifiche e apri il link per confermare l'iscrizione.

Nel Web browser viene visualizzata una risposta di conferma di Amazon SNS.

Per iscriverti all'e-mail di notifica dell' GuardDuty aggiornamento con AWS CLI

1. Esegui il comando riportato qui di seguito con la 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. Nella tua applicazione di posta elettronica, apri il messaggio contenuto in AWS Notifiche e apri il link per confermare l'iscrizione.

Nel Web browser viene visualizzata una risposta di conferma di Amazon SNS.

Formato dei messaggi Amazon SNS

Un esempio di messaggio di notifica GuardDuty generale:

```
{  
  "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-AmazonGuardDutyFullAccess-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"
}

```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```

{
  "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-AmazonGuardDutyFullAccess-v2"
      ]
    }
  ]
}

```

Di seguito è riportato un esempio di messaggio di notifica di GuardDuty aggiornamento relativo a nuovi risultati:

```
{
  "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" : "XWox8GDGLRiCgDOXlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7HpV/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrljlg==",
  "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```
{
  "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."
```

```
  ]]
}
```

Di seguito è riportato un esempio di messaggio di notifica di GuardDuty aggiornamento relativo agli aggiornamenti delle GuardDuty funzionalità:

```
{
  "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```
{
  "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"
  ]]
}

```

Di seguito è riportato un esempio GuardDuty di messaggio di notifica di aggiornamento relativo ai risultati aggiornati:

```

{
  "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"
}

```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```

{
  "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 Quote Amazon

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo diversa indicazione, ogni quota si applica a una Regione specifica. Se per alcune quote è possibile richiedere aumenti, per altre questo non è possibile.

Per visualizzare le quote per GuardDuty, apri la console [Service Quotas](#). Nel riquadro di navigazione, scegli Servizi AWS e seleziona Amazon GuardDuty.

Per richiedere un aumento delle quote, consultare [Richiesta di aumento delle quote](#) nella Guida dell'utente di Service Quotas.

Hai Account AWS le seguenti quote per Amazon GuardDuty per regione.

Note

- Per le quote specifiche di GuardDuty Malware Protection for EC2, consulta. [Quote nella protezione da malware per EC2](#)
- Per le quote specifiche di Malware Protection for S3, vedi. [Quote nella protezione da malware per S3](#)

GuardDuty quote per regione

Risorsa	Default	Commenti
Rilevatori	1	Il numero massimo di risorse del rilevatore che puoi creare per account AWS per regione. Non puoi richieder e un aumento della quota.
Filtri	100	Il numero massimo di filtri salvati per AWS account per regione.

Risorsa	Default	Commenti
		Non puoi richiedere e un aumento della quota.
Ritrovamento del periodo di conservazione	90 giorni	Il numero massimo di giorni di accertamento viene mantenuto. Non puoi richiedere e un aumento della quota.
Indirizzi IP e intervalli CIDR per elenco di indirizzi IP affidabili	2.000	Il numero massimo di indirizzi IP e intervalli CIDR che è possibile includere in un unico elenco di indirizzi IP affidabili. Non puoi richiedere e un aumento della quota.
Indirizzi IP e intervalli CIDR per elenco di indirizzi IP delle minacce	250.000	Il numero massimo di indirizzi IP e intervalli CIDR che è possibile includere in un elenco di indirizzi IP di minaccia. Non puoi richiedere e un aumento della quota.

Risorsa	Default	Commenti
Entità per minaccia, elenco delle entità	1.000	Il numero massimo di entità che è possibile includere in un unico elenco di entità minacciose. Non puoi richiedere e un aumento della quota.
Elenco di entità attendibili	1.000	Il numero massimo di entità che è possibile includere in un elenco di entità attendibili. Non puoi richiedere e un aumento della quota.
Dimensione massima dei file	35 MB	La dimensione massima del file utilizzato per caricare un elenco di entità o un elenco di indirizzi IP. Non puoi richiedere e un aumento della quota.

Risorsa	Default	Commenti
Account membri (su invito)	5000	Il numero massimo di account membri associati a un account amministratore. Non puoi richiedere e un aumento della quota.

Risorsa	Default	Commenti
Account per i membri	50.000	Il numero massimo di account membri associati a un account amministratore attraverso AWS Organizations, inclusi gli account membri che vengono aggiunti all'organizzazione tramite invito. Questo valore predefinito dipende dalla quota corrente per gli account membri in AWS Organizations. Il numero di account membro GuardDuty che vengono aggiunti non AWS Organizations può superare il numero di account membro dell'organizzazione. Per informazioni sul numero di membri Account AWS in un'organizzazione, consulta Valori massimi e minimi nella Guida per l'AWS Organizations utente.

Risorsa	Default	Commenti
Set di informazioni sulle minacce (elenco di indirizzi IP)	6	Il numero massimo di elenchi di indirizzi IP delle minacce che è possibile aggiungere e Account AWS per regione. Non puoi richiedere e un aumento della quota.
Set IP affidabili (elenco di indirizzi IP)	1	Il numero massimo di elenchi di indirizzi IP affidabili che possono essere caricati e attivati Account AWS per ogni regione. Non puoi richiedere e un aumento della quota.
Elenchi di entità minacciose	6	Il numero massimo di elenchi di entità minacciose che è possibile aggiungere e Account AWS per regione. Non puoi richiedere e un aumento della quota.

Risorsa	Default	Commenti
Elenco di entità attendibili	1	Il numero massimo di elenchi di entità attendibili che possono essere caricati e attivati Account AWS per ogni regione. Non puoi richiedere e un aumento della quota.

GuardDuty Supporto per istanze gestite

La tabella seguente indica il supporto offerto dalle GuardDuty varie funzionalità per i diversi tipi di istanze gestite.

Tipo di funzionalità gestita	Supporto per il monitoraggio del runtime	Protezione da malware per il EC2 supporto
Modalità automatica di Amazon EKS	Supportata	Supportata
Istanza AWS Fargate gestita Amazon ECS	Non supportato.	Supportata
Istanza gestita Lambda	Non supportato.	Non supportato.

Risoluzione dei problemi Amazon GuardDuty

Se riscontri problemi relativi all'esecuzione di un'azione specifica di GuardDuty, consulta gli argomenti di questa sezione.

Argomenti

- [Esportazione dei risultati su Amazon S3: errore di accesso](#)
- [Problemi relativi alla protezione da malware per EC2](#)
- [Problemi di monitoraggio del runtime](#)
- [Altre questioni relative alla risoluzione dei problemi](#)

Esportazione dei risultati su Amazon S3: errore di accesso

Quando esporti GuardDuty i risultati in un bucket Amazon S3 (destinazione di pubblicazione), se GuardDuty non riesci ad accedere a questa destinazione di pubblicazione, potresti ricevere un errore di accesso.

Dopo aver configurato le impostazioni per esportare i risultati, se non GuardDuty è possibile esportare i risultati, viene visualizzato un messaggio di errore nella pagina Impostazioni della GuardDuty console. Ciò può accadere potenzialmente quando non è più GuardDuty possibile accedere alla risorsa di destinazione. Ad esempio, se il tuo bucket Amazon S3 è stato eliminato o l'autorizzazione ad accedere al bucket è stata modificata. Ciò può verificarsi anche quando non è più GuardDuty possibile accedere alla AWS KMS chiave utilizzata per crittografare i dati nel bucket Amazon S3. Quando non GuardDuty è in grado di esportare, invia una notifica all'indirizzo e-mail associato all'account per fornire informazioni su questo problema.

Come risolvere l'errore di accesso?

Per risolvere il problema, assicurati che le risorse corrispondenti esistano e GuardDuty disponga delle autorizzazioni per accedere alle risorse necessarie.

Per ulteriori informazioni, consulta [Esportazione dei risultati generati su Amazon S3](#).

Cosa succede se non risolvi questo errore?

Se non risolvi il problema prima del termine del periodo di conservazione dei risultati di 90 giorni GuardDuty, i risultati non verranno esportati. GuardDuty disabiliterà la ricerca delle impostazioni di esportazione per questo account nella regione specifica.

Per ricominciare a esportare i risultati, aggiorna le impostazioni di configurazione nella regione specifica.

Problemi relativi alla protezione da malware per EC2

Questa sezione elenca gli errori che potrebbero verificarsi durante la configurazione o l'utilizzo di Malware Protection for EC2.

Manca l'autorizzazione AWS Organizations di gestione richiesta quando si abilita la scansione GuardDuty antimalware avviata

Se desideri gestire più account utilizzando AWS Organizations e ricevi questo errore `The request failed because you do not have required AWS Organization master permission.`, significa che non hai l'autorizzazione per abilitare la scansione antimalware GuardDuty avviata per più account dell'organizzazione.

Per informazioni sulla concessione delle autorizzazioni all'account di gestione, consulta [Stabilire un accesso affidabile per abilitare la scansione GuardDuty antimalware avviata](#)

All'avvio di una scansione antimalware on demand ricevo un messaggio di un errore che segnala la mancanza delle autorizzazioni richieste.

Se ricevi un errore che suggerisce che non disponi delle autorizzazioni necessarie per avviare una scansione antimalware on demand su un'istanza Amazon EC2, verifica di aver collegato la policy [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#) al tuo ruolo IAM.

Se sei membro di un' AWS organizzazione e continui a ricevere lo stesso errore, connettiti al tuo account di gestione. Per ulteriori informazioni, consulta [AWS Organizations SCP — Accesso negato](#).

Ricevo un **iam:GetRole** errore mentre lavoro con Malware Protection for EC2.

Se ricevi questo errore `Unable to get role:`

`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, significa che non hai l'autorizzazione per abilitare la scansione antimalware GuardDuty avviata o utilizzare la scansione antimalware su richiesta. Verifica di aver collegato la policy [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#) al tuo ruolo IAM.

Sono un account GuardDuty amministratore che deve abilitare la scansione antimalware GuardDuty avviata dall'utente ma non utilizza AWS Managed Policy: to manage. AmazonGuardDutyFullAccess GuardDuty

- Configura il ruolo IAM con cui utilizzi GuardDuty per disporre delle autorizzazioni necessarie per abilitare la scansione GuardDuty antimalware avviata. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [Creazione di un ruolo collegato ai servizi per Malware Protection](#) for EC2.
- Collega [AWS politica gestita: AmazonGuardDutyFullAccess_v2 \(consigliata\)](#) al tuo ruolo IAM. Questo ti aiuterà ad abilitare la scansione GuardDuty antimalware avviata dagli account dei membri.

Problemi di monitoraggio del runtime

Questa sezione elenca gli errori che possono verificarsi durante la configurazione o l'utilizzo del Runtime Monitoring.

Problemi di copertura del runtime

Quando la copertura in fase di esecuzione delle risorse protette diventa inadeguata, la GuardDuty console fornisce il tipo esatto di problema. Dopo aver individuato il tipo di problema, utilizza i seguenti documenti per visualizzare le procedure di risoluzione dei problemi per ogni tipo di risorsa supportato:

- [Risoluzione dei problemi di copertura del runtime di Amazon EC2](#)
- [Risoluzione dei problemi di copertura del runtime di Amazon ECS-Fargate](#)
- [Risoluzione dei problemi di copertura del runtime di Amazon EKS](#)

Risoluzione degli errori di esaurimento della memoria in Runtime Monitoring (solo supporto Amazon EC2)

Questa sezione fornisce le procedure per la risoluzione dei problemi in caso di esaurimento della memoria in base [Limite di CPU e memoria](#) alla distribuzione manuale del GuardDuty Security Agent.

Se systemd interrompe l' GuardDuty agente a causa del out-of-memory problema e si ritiene che fornire più memoria all' GuardDuty agente sia ragionevole, è possibile aggiornare il limite.

1. Con l'autorizzazione root, apri/lib/systemd/system/amazon-guardduty-agent.service.
2. Trova MemoryLimit e MemoryMax aggiorna entrambi i valori.

```
MemoryLimit=256M
MemoryMax=256M
```

3. Dopo aver aggiornato i valori, riavvia l' GuardDuty agente utilizzando il seguente comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Esegui il seguente comando per visualizzare lo stato:

```
sudo systemctl status amazon-guardduty-agent
```

L'output previsto mostrerà il nuovo limite di memoria:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto

Se il GuardDuty contenitore ha contribuito all'errore del flusso di lavoro, vedi. [Risoluzione dei problemi di copertura del runtime di Amazon ECS-Fargate](#) Se il problema persiste, per evitare che il flusso di lavoro non funzioni a causa del GuardDuty contenitore, esegui una delle seguenti operazioni:

- Aggiungi il false tagGuardDutyManaged: al cluster Amazon ECS associato.
- Disattiva la configurazione automatica degli agenti per AWS Fargate (solo ECS) a livello di account. Aggiungi il tag di inclusioneGuardDutyManaged: true al cluster Amazon ECS associato che desideri continuare a monitorare con l'agente GuardDuty automatizzato.

Altre questioni relative alla risoluzione dei problemi

Se non trovi lo scenario adatto al tuo problema, visualizza le seguenti opzioni di risoluzione dei problemi:

- Per problemi generali relativi all'IAM quando accedi a <https://console.aws.amazon.com/guardduty/>, consulta [Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon](#).
- Per problemi di autenticazione e autorizzazione durante l'accesso AWS AWS Console Home, consulta [Risoluzione dei problemi di IAM](#).

GuardDuty Regioni ed endpoint Amazon

Per visualizzare Regioni AWS dove GuardDuty è disponibile Amazon, consulta [Amazon GuardDuty endpoints](#) nel Riferimenti generali di Amazon Web Services.

Ti consigliamo di abilitare tutte le GuardDuty funzionalità supportate Regioni AWS. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche nelle Regioni che non utilizzi attivamente. Ciò consente inoltre di GuardDuty monitorare AWS CloudTrail gli eventi per il soggetto supportato Regioni AWS, riducendo la sua capacità di rilevare attività che coinvolgono servizi globali.

Disponibilità di funzionalità specifiche per ogni regione

Un elenco di differenze regionali per specificare la disponibilità delle GuardDuty funzionalità.

ListFindings e GetFindingsStatistics APIs

I [GetFindingsStatisticse](#) [ListFindings](#) APIs hanno una consoleOnly bandiera temporanea. Quando si utilizzano uno o entrambi APIs, il consoleOnly flag indica che l'API può recuperare risultati fino a un limite massimo di 1000.

Protezione da malware per EC2

GuardDuty supporta la [Protezione da malware per EC2](#) funzionalità nelle [AWS Dedicated Local Zones](#).

Protezione RDS

La protezione RDS non è supportata nella regione Asia Pacifico (Taipei) (). ap-east-2

Tipo di ricerca IAM: [CredentialAccess:IAMUser/CompromisedCredentials](#)

Il tipo di CompromisedCredentials ricerca CredentialAccess:IAMUser/non è supportato nelle seguenti regioni.

Regione AWS	Codice regione
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1

Regione AWS	Codice regione
Cina (Pechino)	cn-north-1
China (Ningxia)	cn-northwest-1

Tipo di ricerca IAM: [DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)

Il tipo di BedrockLoggingDisabled ricerca DefenseEvasion:IAMUser/non è supportato nella regione Asia Pacifico (Hong Kongap-east-1) ().

Supporto API generale

Quanto segue APIs nell'Amazon GuardDuty API Reference può presentare differenze regionali a causa dell'indisponibilità di alcune fonti di dati o funzionalità specificate Regioni AWS in precedenza:

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)
- [GetDetector](#)
- [GetMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

Tipi di esiti di Amazon EC2: [DefenseEvasion:EC2/UnusualDoHActivity](#) e [DefenseEvasion:EC2/UnusualDoTActivity](#)

La tabella seguente mostra Regioni AWS dove GuardDuty è disponibile, ma questi due tipi di ricerca di Amazon EC2 non sono ancora supportati.

Regione AWS	Codice regione
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Giacarta)	ap-southeast-3

AWS GovCloud (US) Regioni

Per le informazioni più recenti, consulta [Amazon GuardDuty](#) nella Guida AWS GovCloud (US) per l'utente.

Regioni della Cina

Per le informazioni più recenti, consulta [Differenze nella disponibilità e nell'implementazione delle funzionalità](#).

GuardDuty azioni e parametri precedenti

Amazon GuardDuty ha reso obsolete alcune azioni e parametri dell'API, ma le supporta ancora. La best practice consiste nell'utilizzare le nuove azioni e parametri API che sostituiscono le opzioni legacy. Nella tabella seguente vengono confrontate le operazioni e i parametri legacy e quelli nuovi.

Operazioni/ parametri legacy	Operazioni/parametri nuovi	Confronto
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Con la stessa implementazione in entrambe le azioni, GuardDuty utilizza il termine in. Administrator DisassociateFromAdministratorAccount
autoEnable e parametro in DescribeOrganizationConfigurationUpdateOrganizationConfiguration	autoEnableOrganizationMembers	Con autoEnableOrganizationMembers , l'account GuardDuty amministratore può controllare e applicare GuardDuty per tutti gli account membri uno dei valori. Utilizzando il APIs, potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri. Per ulteriori informazioni sui possibili valori del autoEnableOrganizationMembers campo, vedi autoEnableOrganizationMembers
dataSourcees parametro APIs elencato in GuardDuty Modifiche all'API a marzo 2023 .	features	A partire da marzo 2023, è possibile configurare GuardDuty Protezione da malware per EC2 e utilizzare i nuovi piani di GuardDuty protezione e features. I piani di protezione sono stati lanciati prima di marzo 2023, tra cui Malware Protection for supporta EC2 ancora la configura

Operazioni/ parametri legacy	Operazioni/parametri nuovi	Confronto
		zione tramite <code>dataSources</code> . Se si utilizza APIs per configurare un piano di protezione, ogni richiesta API può includere <code>dataSources</code> o <code>features</code> non entrambi.

Cronologia dei documenti per Amazon GuardDuty

La tabella seguente descrive importanti modifiche alla documentazione dall'ultima versione della Amazon GuardDuty User Guide. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile iscriversi a un feed RSS.

Modifica	Descrizione	Data
Funzionalità aggiornata - Runtime Monitoring	GuardDuty Runtime Monitoring rilascia la nuova versione 1.9.2 del security agent per le risorse Amazon EC2. Per ulteriori informazioni sulle nuove versioni degli agenti e un elenco di risorse aggiuntive e per aggiornare il security agent, consulta Security Agent GuardDuty Release versions.	3 aprile 2026
Aggiornato AmazonGuardDutyServiceRolePolicy	È stata aggiunta l'cloudtrail:CreateServiceLinkedChannel autorizzazione per abilitare un meccanismo aggiuntivo per la fruizione AWS CloudTrail degli eventi. Per ulteriori informazioni, consulta GuardDuty gli aggiornamenti delle politiche AWS gestite .	25 marzo 2026
Funzionalità aggiornata: monitoraggio del runtime	GuardDuty Runtime Monitoring Aggiunto supporto per Kubernetes versione 1.35. Per ulteriori informazioni, consulta Prerequisiti per il monitoraggio del runtime.	20 marzo 2026

[La nuova policy di accesso completa e ad ambito ridotto AmazonGuardDutyFullAccess_v2](#) [sostituisce AmazonGuardDutyFullAccess](#).

A partire dal 13 marzo 2026, GuardDuty ha reso obsoleta la AmazonGuardDutyFullAccess politica e l'ha sostituita con una politica limitata denominata AmazonGuardDutyFullAccess_v2. [Per ulteriori informazioni, consulta managed policy: _v2.AWS AmazonGuardDutyFullAccess](#)

13 marzo 2026

[Nuovo tipo di reperto - CredentialAccess:IAMUser/CompromisedCredentials](#)

GuardDuty Introduce un nuovo tipo di ricerca che rileva quando una chiave di accesso IAM ritenuta potenzialmente compromessa viene utilizzata per richiamare le operazioni API in. AWS [Per ulteriori informazioni, vedere:/. CredentialAccess IAMUser CompromisedCredentials](#)

6 marzo 2026

[Nuovo tipo di reperto - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)

GuardDuty introduce un nuovo tipo di ricerca che rileva quando un host esterno AWS tenta di eseguire operazioni AWS API utilizzando AWS credenziali temporanee create su una AWS Lambda risorsa dell'ambiente. AWS Per ulteriori informazioni, consulta [UnauthorizedAccess : IAMUser/.outsideAWS. ResourceCredentialExfiltration](#)

16 dicembre 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitorin
g rilascia la nuova versione
1.9.1 del Security Agent per
le risorse Amazon EC2. Per
ulteriori informazioni sulle
nuove versioni degli agenti e
un elenco di risorse aggiuntiv
e per aggiornare il security
agent, consulta Security Agent
[GuardDuty Release](#) versions.

2 dicembre 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitorin
g rilascia la nuova versione
1.12.1 del security agent per
le risorse Amazon EKS. Per
ulteriori informazioni sulla
nuova versione dell'agente e
un elenco di risorse aggiuntiv
e per aggiornare il security
agent, consulta le versioni di
[rilascio del GuardDuty security
agent](#).

2 dicembre 2025

Funzionalità aggiornata: rilevamento esteso delle minacce

GuardDuty Extended Threat Detection introduce due nuovi tipi di ricerca delle sequenze di attacco, [:EC2/AttackSequence](#) e [:ECS/CompromisedInstanceGroup](#), che aiutano a [AttackSequence](#) rilevare attacchi in [CompromisedCluster](#) più fasi che coinvolgono istanze [Amazon EC2](#) e cluster Amazon ECS compromessi. Abilita [il monitoraggio](#) del runtime per massimizzare il rilevamento delle minacce. Per ulteriori informazioni, consulta [Tipi di ricerca della sequenza di attacco](#).

2 dicembre 2025

Nuova funzionalità: Wildcard in Suppression Rules

GuardDuty ha migliorato le sue capacità di soppressione con l'introduzione di Matches and NotMatches Conditions che supportano i caratteri jolly. I clienti possono ora usare* (per abbinare un numero qualsiasi di caratteri) e? (per corrispondere al massimo a 1 carattere) come jolly durante la creazione delle regole di soppressione. Regole di [soppressione](#).

2 dicembre 2025

[Nuova funzionalità: Amazon CloudWatch Usage Metrics Support](#)

GuardDuty introduce le metriche di utilizzo della pubblicazione in Amazon CloudWatch per tutti i piani di protezione, consentendo ai clienti di monitorare l'utilizzo. Per ulteriori informazioni, consulta [Monitoraggio dell' GuardDuty utilizzo e stima dei costi](#)

25 novembre 2025

[Nuovo tipo di reperto - DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)

GuardDuty introduce un nuovo tipo di rilevamento che rileva quando la registrazione delle invocazioni del modello Amazon Bedrock è disabilitata, il che può indicare tentativi di eludere il rilevamento dell'attività del carico di lavoro AI. [Per ulteriori informazioni, consulta: /. DefenseEvasion IAMUser BedrockLoggingDisabled](#)

21 novembre 2025

[Nuova funzionalità: protezione da malware per il backup](#)

GuardDuty Malware Protection for Backup è ora disponibile in tutte le aree commerciali in cui GuardDuty è disponibile. Questa funzionalità consente di rilevare la potenziale presenza di malware nelle risorse di backup attraverso scansioni complete e incrementali di snapshot di Amazon EBS, EC2 AMIs e punti di ripristino. Per ulteriori informazioni su questa funzionalità, vedere [Malware Protection for Backup](#)

19 novembre 2025

[Passa a AmazonGuardDutyFullAccess e AmazonGuardDutyFullAccess_V2](#)

È stata aggiunta l'autorizzazione che consente di passare un ruolo IAM a GuardDuty quando si attiva Malware Protection for Backup.

19 novembre 2025

[Nuova funzionalità: protezione da malware per la scansione su richiesta di S3.](#)

GuardDuty annuncia Scan on Demand for Malware Protection per S3. Utilizzando questa funzionalità puoi utilizzare la nuova SendObjectMalwareScan API per attivare scansioni su qualsiasi oggetto già esistente archiviato nei tuoi bucket S3. Per informazioni, consulta la scansione antimalware [S3 su richiesta](#).

17 novembre 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitorin
g rilascia la nuova versione
1.9.0 del Security Agent per
le risorse Amazon ECS.AWS
Fargate Per informazioni sulle
nuove versioni degli agenti e
un elenco di risorse aggiuntiv
e per aggiornare il security
agent, consulta Security Agent
[GuardDuty Release](#) versions.

28 ottobre 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitorin
g rilascia la nuova versione
1.9.0 del Security Agent per
le risorse Amazon EC2. Per
informazioni sulle nuove
versioni degli agenti e un
elenco di risorse aggiuntiv
e per aggiornare il security
agent, consulta Security Agent
[GuardDuty Release](#) versions.

23 ottobre 2025

Nuovo tipo di risultato
di Runtime Monitoring -
DefenseEvasion:Runtime/Kern
elModuleLoaded

GuardDuty Runtime Monitorin
g introduce un nuovo tipo di
ricerca che aiuta a identific
are le tecniche di evasione
della difesa in cui gli autori
delle minacce utilizzano i
moduli del kernel per aggirare i
controlli di sicurezza, modificar
e le operazioni di sistema e
ottenere un accesso persisten
te al sistema. [Per ulteriori
informazioni, vedi:runtime/.
DefenseEvasion KernelMod
uleLoaded](#)

15 ottobre 2025

Funzionalità aggiornata:
monitoraggio del runtime

È stato aggiunto il supporto per la versione 1.34 di Kubernetes per le distribuzioni del sistema operativo e la versione del security agent per le risorse Role GuardDuty SageMaker Manager for Amazon EKS. Per ulteriori informazioni, consulta [Convalida dei requisiti architetturali per Amazon EKS](#).

3 ottobre 2025

Sono state aggiunte linee guida per la risoluzione dei problemi del database Amazon RDS

Sono state aggiunte linee guida per la risoluzione dei problemi del database RDS che possono influire sulle funzionalità di monitoraggio di GuardDuty RDS Protection, inclusi storage-full lo stato e i requisiti di replica di lettura RDS per PostgreSQL. [Per ulteriori informazioni, consulta Risoluzione dei problemi di monitoraggio di RDS Protection](#).

15 settembre 2025

Funzionalità aggiornata: monitoraggio del runtime	Aggiunta la distribuzione del sistema operativo Ubuntu Noble con supporto per le versioni del kernel 6.13 e 6.14 per GuardDuty Runtime Monitoring for Amazon EC2. Per informazioni sulla versione dell'agente EC2 supportata per questa distribuzione del sistema operativo, consulta Convalida dei requisiti architetturali per Amazon EC2.	13 settembre 2025
Funzionalità aggiornata: protezione RDS	È stato aggiunto il supporto PostgreSQL 17 per RDS per i database PostgreSQL monitorati da RDS Protection. GuardDuty Per ulteriori informazioni, consulta Database supportati in RDS Protection.	13 settembre 2025
Funzionalità aggiornata: protezione da malware per S3	GuardDuty Malware Protection for S3 aumenta la quota predefinita dei file di archivio estratti da 1.000 a 10.000 file. Per ulteriori informazioni, consulta Quotas in Malware Protection for S3.	3 settembre 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitoring rilascia la nuova versione 1.11 del security agent per le risorse Amazon EKS. Per ulteriori informazioni sulla nuova versione dell'agente e un elenco di risorse aggiuntive e per aggiornare il security agent, consulta [le versioni di rilascio del GuardDuty security agent](#).

29 agosto 2025

Funzionalità aggiornata:
utilizzo degli elenchi

GuardDuty introduce elenchi personalizzati di entità affidabili e minacciate che supportano sia gli indirizzi IP che i nomi di dominio. GuardDuty continua a supportare l'elenco di indirizzi IP e consiglia di utilizzare l'elenco di entità per il rilevamento personalizzato delle minacce. Per ulteriori informazioni, vedere [Personalizzazione del rilevamento delle minacce con elenchi di entità ed elenchi di indirizzi IP](#).

15 agosto 2025

Funzionalità aggiornata - Runtime Monitoring

GuardDuty Runtime Monitoring rilascia la nuova versione 1.8.0 del Security Agent per le risorse Amazon EC2 e Amazon AWS Fargate ECS-. [Per ulteriori informazioni sulle nuove versioni degli agenti e un elenco di risorse aggiuntive per aggiornare il security agent, consulta Security Agent Release GuardDuty versions.](#)

12 agosto 2025

Supporto per la regione Asia Pacifico (Taipei)

Amazon GuardDuty è ora disponibile nella regione Asia Pacifico (Taipei) (ap-east-2). Per abilitarlo GuardDuty in questa regione, consulta [Guida introduttiva](#). Puoi ricevere notifiche sugli aggiornamenti delle GuardDuty funzionalità e sui rilevamenti delle minacce [iscrivendoti agli annunci di Amazon GuardDuty SNS](#) in questa regione.

31 luglio 2025

Funzionalità aggiornata: protezione da malware per S3

Malware Protection for S3 ora supporta la scansione di oggetti fino a 100 GB, rispetto ai 5 GB precedenti. Ciò include sia i singoli oggetti che i file di archivio estratti. Per ulteriori informazioni, consulta [Malware Protection for S3 Quotas](#).

23 luglio 2025

[Funzionalità aggiornata: è stato aggiunto il proprietario previsto del bucket negli elenchi di indirizzi IP e minacce attendibili](#)

GuardDuty ha aggiunto il campo Expected bucket owner per gli elenchi di IP affidabili e di minacce. In questo campo facoltativo, puoi specificare un Account AWS ID da utilizzare per verificare la proprietà del bucket Amazon S3. GuardDuty Per ulteriori informazioni, vedere [Utilizzo degli elenchi di IP attendibili e degli elenchi delle minacce](#).

16 luglio 2025

[Funzionalità aggiornata: rilevamento esteso delle minacce](#)

GuardDuty Extended Threat Detection ora amplia il supporto per i cluster Amazon EKS correlando più segnali di sicurezza tra i log di controllo EKS, il comportamento di runtime dei processi e l'attività delle API. AWS [Abilita EKS Protection, Runtime Monitoring \(con il componente aggiuntivo EKS\) o entrambi per massimizzare il rilevamento delle minacce](#). [Per identificare potenziali minacce, GuardDuty introduce un nuovo tipo di ricerca —:EKS/. AttackSequence CompromisedCluster](#) [Per ulteriori informazioni, vedere Extended Threat Detection](#).

17 giugno 2025

Funzionalità aggiornata:
protezione da malware per S3

Malware Protection for S3 non supporta la scansione di archivi con un rapporto di compressione estremamente elevato. Questi file verranno ignorati durante la scansione e contrassegnati con il risultato della scansione di UNSUPPORTED. Per ulteriori informazioni, consulta lo stato [potenziale della scansione degli oggetti S3 e lo stato dei risultati](#).

13 giugno 2025

Funzionalità aggiornata:
protezione da malware per EC2

Malware Protection for EC2 ha aggiunto il supporto per la scansione della maggior parte delle istanze con as. productCode marketplace. Ciò vale sia per le scansioni GuardDuty antimalware avviate che per le scansioni antimalware su richiesta. Per ulteriori informazioni, consulta [Motivi per ignorare](#) una risorsa durante la scansione antimalware.

13 giugno 2025

[Nuova politica AmazonGuardDutyFullAccess_v2](#)

È stata aggiunta una nuova AmazonGuardDutyFullAccess_v2 politica con autorizzazioni per migliorare la sicurezza limitando le azioni amministrative ai responsabili del servizio. GuardDuty Per informazioni su questa politica consigliata, vedi policy [AWS gestita](#): AmazonGuardDutyFullAccess_v2

4 giugno 2025

[Supporto regionale esteso per la protezione RDS](#)

GuardDuty La protezione RDS è ora disponibile nelle regioni di Messico (Centrale), Asia Pacifico (Tailandia) e Asia Pacifico (Malesia). RDS Protection ti aiuta a rilevare comportamenti di accesso potenzialmente sospetti in Aurora MySQL, Aurora PostgreSQL (incluso Limitless Database) e RDS for PostgreSQL supportati. In caso di GuardDuty rilevamento di minacce, genera un risultato di protezione RDS. Per ulteriori informazioni sui database supportati e sull'attivazione di questo piano di protezione nelle nuove regioni supportate, consulta [RDS Protection](#).

4 giugno 2025

[Funzionalità aggiornata:
monitoraggio del runtime](#)

GuardDuty Runtime Monitorin
g rilascia la nuova versione
1.7.1 del Security Agent per
le risorse Amazon EC2. Per
ulteriori informazioni sulle
nuove versioni degli agenti e
un elenco di risorse aggiuntiv
e per aggiornare il security
agent, consulta Security Agent
[GuardDuty Release](#) versions.

3 giugno 2025

[Support per il rilevamento
esteso delle minacce](#)

GuardDuty Extended Threat
Detection è ora disponibile in
Asia Pacifico (Tailandia) (ap-
southeast-7). Senza necessità
di attivazione, rileva attacchi
in più fasi che riguardano fonti
di dati, diversi tipi di risorse e
tempi, all'interno di AWS un
unico. Account AWS Quando
vengono rilevate potenziali
minacce, genera una ricerca
della sequenza di attacco. Per
ulteriori informazioni, consulta
[Extended Threat Detection](#).

12 maggio 2025

[Supporto per la regione del Messico \(Centrale\)](#)

Amazon GuardDuty è ora disponibile nella regione Messico (Centrale) mx-central-1 (). Per abilitarlo GuardDuty in questa regione, consulta [Guida introduttiva](#). Puoi ricevere notifiche sugli aggiornamenti delle GuardDuty funzionalità e sui rilevamenti delle minacce [iscrivendoti agli annunci di Amazon GuardDuty SNS](#) in questa regione.

07 maggio 2025

[Funzionalità aggiornata - Runtime Monitoring](#)

GuardDuty Runtime Monitoring rilascia la nuova versione 1.10.0 del Security Agent per le risorse Amazon EKS. Per ulteriori informazioni sulle nuove versioni degli agenti e un elenco di risorse aggiuntive e per aggiornare il security agent, consulta GuardDuty Security Agent [Release versions](#).

4 aprile 2025

Funzionalità aggiornata - Runtime Monitoring

GuardDuty Runtime Monitoring rilascia il nuovo agente di sicurezza versione 1.7.0 per le risorse Amazon ECS-Fargate. [Per ulteriori informazioni sulle nuove versioni degli agenti e un elenco di risorse aggiuntive per aggiornare il security agent, consulta GuardDuty Security Agent Release versions.](#)

4 aprile 2025

Funzionalità aggiornata - Runtime Monitoring

GuardDuty Runtime Monitoring rilascia la nuova versione 1.7.0 del Security Agent per le risorse Amazon EC2. Per ulteriori informazioni sulle nuove versioni degli agenti e un elenco di risorse aggiuntive e per aggiornare il security agent, consulta [Security Agent GuardDuty Release versions](#).

03 aprile 2025

Supporto per la regione Asia Pacifico (Tailandia)

Amazon GuardDuty è ora disponibile nella regione Asia Pacifico (Tailandia). Per informazioni sulle funzionalità supportate in questa regione, consulta [Disponibilità delle funzionalità specifiche per regione](#). Per abilitarle GuardDuty in questa regione, consulta [Guida introduttiva](#). Puoi ricevere notifiche sugli aggiornamenti delle GuardDuty funzionalità e sui rilevamenti delle minacce [iscrivendoti agli annunci di Amazon GuardDuty SNS](#).

1 aprile 2025

Funzionalità aggiornate

La dashboard di riepilogo ora mostra informazioni dettagliate basate su tutti i risultati di sicurezza generati, eliminando il precedente vincolo di 5.000 risultati. Per informazioni su queste informazioni, consulta la dashboard di [GuardDuty riepilogo](#).

17 marzo 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitorin
g rilascia la nuova versione
1.9.0 del security agent per
le risorse Amazon EKS. Per
ulteriori informazioni sulle
nuove versioni degli agenti e
un elenco di risorse aggiuntiv
e per aggiornare il security
agent, consulta GuardDuty
Security Agent [Release
versions](#).

2 marzo 2025

Funzionalità aggiornata:
monitoraggio del runtime

GuardDuty Runtime Monitorin
g ha aggiunto un nuovo tipo di
problema di copertura (Agent
Not Provisioned) per le risorse
Amazon EC2. Per informazi
oni sulla risoluzione di questo
problema, consulta [Risoluzio
ne dei problemi di copertura
del runtime di Amazon EC2](#).

21 febbraio 2025

Funzionalità aggiornata -
Runtime Monitoring

GuardDuty Runtime Monitorin
g rilascia nuovi agenti di
sicurezza per le risorse
Amazon EC2 e Amazon ECS-
Fargate. [Per ulteriori informazi
oni sulle nuove versioni degli
agenti e un elenco di risorse
aggiuntive per aggiornare
i security agent, consulta
Security Agent Release
GuardDuty versions](#).

6 febbraio 2025

[GuardDuty supporto nell'attuale regione Asia-Pacifico \(Malesia\)](#)

GuardDuty Extended Threat Detection è ora disponibile nella regione Asia Pacifico (Malesia). Per ulteriori informazioni, consulta [Extended Threat Detection](#).

28 gennaio 2025

[Supporto per la regione Asia Pacifico \(Malesia\)](#)

Amazon GuardDuty è ora disponibile nella regione Asia Pacifico (Malesia). Per informazioni sulle funzionalità supportate in questa regione, consulta [Disponibilità delle funzionalità specifiche per regione](#). Per abilitarle GuardDuty in questa regione, consulta [Guida introduttiva](#). Puoi ricevere notifiche sugli aggiornamenti delle GuardDuty funzionalità e sui rilevamenti delle minacce [iscrivendoti agli annunci di Amazon GuardDuty SNS](#).

16 gennaio 2025

Funzionalità aggiornata - Runtime Monitoring

GuardDuty Runtime Monitoring ha aggiornato informazioni aggiuntive e procedure di risoluzione dei problemi di copertura di Amazon ECS-Fargate associati all'agente non fornito. Per ulteriori informazioni sul tipo di problema Agent not provisioned, consulta [Risoluzione dei problemi di copertura del runtime di Amazon ECS-Fargate](#).

08 gennaio 2025

Nuovo tipo di ricerca - Policy:IAMUser/ShortTermRootCredentialUsage

GuardDuty introduce un nuovo tipo di ricerca che avvisa l'utente quando le credenziali utente con restrizioni, create per gli utenti elencati Account AWS nell'ambiente, vengono utilizzate per effettuare richieste a. Servizi AWS Per ulteriori informazioni, vedere [Policy:/. IAMUser ShortTermRootCredentialUsage](#)

08 gennaio 2025

[Nuova funzionalità: rilevamento GuardDuty esteso delle minacce](#)

GuardDuty annuncia Extended Threat Detection per rilevare sequenze di attacco in più fasi che riguardano fonti di dati e AWS risorse GuardDuty fondamentali dell'azienda Account AWS, in un periodo di tempo specifico. Senza costi aggiuntivi, questa funzionalità viene abilitata automaticamente per tutti gli account abilitati. GuardDuty Questa funzionalità annuncia due nuovi tipi di GuardDuty ricerca, denominati [Attack sequence finding types](#). Per ulteriori informazioni, consulta [Extended Threat Detection](#).

1 dicembre 2024

[Funzionalità multiservizio migliorata: monitoraggio del runtime e protezione da malware per EC2](#)

Impatto delle nuove funzionalità di Amazon Elastic Kubernetes Service (Amazon EKS) sulle funzionalità di Amazon: GuardDuty

1 dicembre 2024

- Amazon EKS Auto Mode: supporta sia il Runtime Monitoring per Amazon EKS che Malware Protection for EC2.
- Nodi ibridi Amazon EKS: sia il monitoraggio del runtime per Amazon EKS che la protezione da malware per EC2 non supportano questa funzionalità.

Per ulteriori informazioni, consulta [Come funziona il monitoraggio del runtime con i cluster Amazon EKS e Malware Protection for EC2.](#)

[Funzionalità aggiornate in Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.8.1 (v1.8.1-eks-build.2) per le risorse Amazon EKS. Con questa nuova versione agente, GuardDuty estende il supporto di Runtime Monitoring per le risorse Amazon EKS che funzionano su RedHat CentOS e Fedora. Per ulteriori informazioni, consulta [Convalida](#) dei requisiti architetturali. Per informazioni sulle note di rilascio, consulta [l'agente GuardDuty di sicurezza per le risorse di Amazon EKS](#).

23 novembre 2024

[Funzionalità aggiornate in Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.5.0 per le risorse Amazon EC2. Con questa nuova versione agente, GuardDuty estende il supporto di Runtime Monitoring per le risorse Amazon EC2 che funzionano su RedHat CentOS e Fedora. [Per ulteriori informazioni, consulta Convalida dei requisiti architetturali](#). Per informazioni sulle note di rilascio, consulta [l'agente GuardDuty di sicurezza per le risorse di Amazon EC2](#).

20 novembre 2024

[Funzionalità aggiornate nel monitoraggio del runtime - Amazon ECS-Fargate](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.5.0 per le risorse Amazon ECS-Fargate. Per ulteriori informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for AWS Fargate \(solo Amazon ECS\)](#).

14 novembre 2024

[Funzionalità aggiornata in Malware Protection for EC2](#)

GuardDuty Malware Protection for EC2 ha aggiunto tre tipi di risultati di Runtime Monitoring all'elenco dei [risultati che richiamano la scansione del malware GuardDuty avviata dalle istanze Amazon](#) EC2. Gli account che hanno abilitato Malware Protection for EC2 osserveranno la scansione del malware GuardDuty avviata quando genera uno dei seguenti risultati: GuardDuty

7 novembre 2024

- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[Funzionalità aggiornate in RDS Protection](#)

6 novembre 2024

GuardDuty RDS Protection aggiunge la nuova versione del motore di database [Aurora PostgreSQL](#) Limitless all'elenco dei database supportati.

16.4-limitless Se hai già abilitato RDS Protection, GuardDuty inizierà automaticamente a monitorare il comportamento di accesso per il Limitless Database. Account AWS Gli account che hanno già utilizzato la prova gratuita di 30 giorni per RDS Protection dovranno sostenere i costi di utilizzo associati a Limitless Database, insieme ad altri database supportati monitorati. [Per ulteriori informazioni, consulta RDS Protection.](#)

[Espansione GuardDuty e AWS PrivateLink integrazione della regione](#)

GuardDuty ora estende il supporto regionale per [Amazon GuardDuty e gli endpoint VPC di interfaccia](#) ().AWS PrivateLink In precedenza, il supporto regionale era disponibile per Stati Uniti orientali (Virginia settentrionale), Europa (Irlanda) e Israele (Tel Aviv). Questo supporto è ora esteso a tutti i paesi Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni sulle differenze regionali, consulta [Disponibilità delle funzionalità specifiche per regione](#).

6 novembre 2024

[Funzionalità aggiornate nel monitoraggio del runtime - Amazon ECS-Fargate](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.1 per le risorse Amazon ECS-Fargate. Per ulteriori informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for AWS Fargate \(solo Amazon ECS\)](#).

24 ottobre 2024

[È stato aggiunto il supporto per le operazioni di GuardDuty CloudFormation tag](#)

GuardDuty ora supporta l'aggiornamento della chiave e del valore dei tag e dei tag a livello di stack. A tale scopo, aggiungi l'autorizzazione `guardduty:tagResources` al ruolo IAM. Per informazioni in merito GuardDuty CloudFormation, consulta il [riferimento ai tipi di GuardDuty risorse Amazon](#) nella Guida AWS CloudFormation per l'utente.

24 ottobre 2024

[Funzionalità aggiornata in GuardDuty Malware Protection for S3](#)

Quando abiliti la protezione da malware per S3, puoi scegliere un ruolo di servizio con le autorizzazioni necessarie per eseguire azioni di scansione antimalware per tuo conto. Per ulteriori informazioni sull'attivazione di Malware Protection for S3, consulta [Configurazione della protezione da malware per S3 per il bucket S3](#).

22 ottobre 2024

Funzionalità aggiornate

21 ottobre 2024

GuardDuty migliora il tipo di [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#) ricerca per rilevare l'uso delle credenziali dell' AWS istanza Amazon EC2 dagli AWS PrivateLink endpoint VPC (Account AWS) che non sono associati al ruolo dell'istanza Amazon EC2. Questa nuova GuardDuty funzionalità rileva il potenziale uso improprio delle credenziali dell'istanza Amazon EC2 e fornisce un contesto del Account AWS telecomando utilizzando le credenziali di sessione che esfiltrano. Per ulteriori informazioni sugli endpoint di AWS servizio supportati da questo nuovo rilevamento, consulta la sezione [Registrazione](#) degli eventi delle attività di rete nella Guida per l'utente. AWS CloudTrail

[Funzionalità aggiornata:
monitoraggio del runtime
GuardDuty](#)

GuardDuty Runtime Monitoring ha aggiunto i seguenti tre tipi di risultati che ti avvisano quando vengono eseguiti comandi sospetti su un'istanza Amazon EC2 o un carico di lavoro di container all'interno del tuo ambiente: AWS

10 ottobre 2024

- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

[Nuova funzionalità - Aggiunto
il supporto per gli endpoint
VPC](#)

GuardDuty è ora integrato AWS PrivateLink e supporta gli endpoint VPC. Per ulteriori informazioni sull'AWS PrivateLink integrazione, consulta [Amazon GuardDuty e interfaccia VPC endpoint \(\)](#).AWS PrivateLink

17 settembre 2024

[Funzionalità aggiornate in
Runtime Monitoring - Amazon
EKS](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.7.1 per le risorse Amazon EKS. Per ulteriori informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for Amazon EKS](#).

13 settembre 2024

[Funzionalità aggiornata in
Malware Protection for S3](#)

Malware Protection for S3 ha aggiunto un nuovo campo allo `s3Throttled` schema Amazon EventBridge (EventBridge) dei risultati della scansione degli oggetti S3. Il `s3Throttled` campo indica se si è verificato un ritardo nel caricamento o nel recupero dello storage dai bucket Amazon Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon](#). EventBridge

13 settembre 2024

[Funzionalità aggiornate in
Runtime Monitoring - Amazon
EC2](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.1 per le risorse Amazon EC2. Per ulteriori informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for Amazon EC2](#).

12 settembre 2024

[Funzionalità aggiornate nel
monitoraggio del runtime -
Amazon ECS-Fargate](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.1 per le risorse Amazon ECS-Fargate. Per ulteriori informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for AWS Fargate \(solo Amazon ECS\)](#).

11 settembre 2024

[Ruolo GuardDuty collegato al servizio \(SLR\) aggiornato](#)

GuardDuty ha aggiornato la reflex per includere l'ec2:DescribeVpcs autorizzazione nelle azioni di Amazon EC2. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi per GuardDuty](#).

22 agosto 2024

[Significativa aggiunta di contenuti](#)

GuardDuty ha aggiunto importanti aggiornamenti di contenuto alla funzionalità Malware Protection for S3.

20 agosto 2024

- Sono stati aggiunti nuovi esempi di schema di notifica di esempio per configurare EventBridge le regole di Amazon per ricevere notifiche relative allo stato delle risorse del piano Malware Protection e ai risultati della scansione degli oggetti S3. Per ulteriori informazioni, consulta [Monitoraggio delle scansioni di oggetti S3 con Amazon EventBridge](#)
- Sono state aggiunte informazioni sulla [risoluzione dei problemi relativi agli errori dei tag post-scansione degli oggetti S3](#).

[Funzionalità aggiornate in GuardDuty Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 per le risorse Amazon EC2. Per ulteriori informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for Amazon EC2](#).

19 agosto 2024

[Funzionalità aggiornate in GuardDuty Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.7.0 per le risorse Amazon EKS. Per ulteriori informazioni sulle note di rilascio, consulta [l'agente GuardDuty di sicurezza per i cluster Amazon EKS](#).

17 agosto 2024

[Significativa aggiunta di contenuti](#)

GuardDuty ha aggiunto nuove informazioni sulla metodologia di rilevamento del malware e sui motori di scansione utilizzati per le funzionalità Malware Protection for S3 e Malware Protection for EC2. Per ulteriori informazioni, consulta il motore di scansione per il [rilevamento del GuardDuty malware](#).

15 agosto 2024

[Nuova funzionalità - Protezione
e dei carichi di lavoro di
intelligenza artificiale](#)

GuardDuty il rilevamento delle minacce di base e la protezione Lambda ti aiutano a proteggere e rilevare meglio le minacce ai carichi di lavoro di intelligenza artificiale su cui si basano. AWS Per ulteriori informazioni, consulta [Proteggere i carichi di lavoro AI](#) con. GuardDuty

14 agosto 2024

[Funzionalità aggiornata in
GuardDuty Runtime Monitorin
g - Fargate \(solo Amazon
ECS\)](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 per le risorse AWS Fargate (solo Amazon ECS). Per ulteriori informazioni sulle note di rilascio, vedere [GuardDuty Security Agent for Fargate-ECS](#).

9 agosto 2024

[Funzionalità aggiornata:
protezione da malware per S3](#)

GuardDuty Malware Protection for S3 aumenta la quota del numero massimo di bucket S3 da 10 a 25 bucket. Questa quota si applica a uno per ciascuno. Account AWS Regione AWS Per ulteriori informazioni, consulta [Malware Protection for S3](#).

8 agosto 2024

[Aggiornato: nuovi tipi di ricerca in Runtime Monitoring](#)

GuardDuty ha aggiunto due nuovi tipi di ricerca di Runtime Monitoring che consentono di rilevare le minacce che comportano la creazione di shell sospette sulla risorsa monitorata e l'escalation dei privilegi, quando un processo eleva in modo sospetto i propri privilegi a root.

6 agosto 2024

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[Aggiornato: integrazione con AWS Security Hub CSPM](#)

AWS Security Hub CSPM fornisce un elenco di controlli di GuardDuty sicurezza per valutare le risorse e verificarne la conformità rispetto agli standard e alle best practice del settore della sicurezza. Per ulteriori informazioni, vedere [Utilizzo GuardDuty dei controlli in Security Hub CSPM](#).

11 luglio 2024

[Script GuardDuty tester aggiornato per i risultati](#)

GuardDuty ora supporta oltre 100 risultati con diverse AWS risorse in un account dedicato. Per ulteriori informazioni, consulta [GuardDuty Risultati dei test in account dedicati](#).

28 giugno 2024

Funzionalità aggiornata in Runtime Monitoring

Runtime Monitoring ha rilasciato o una nuova versione del security agent 1.2.0 per la risorsa Amazon EC2. Per informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for Amazon EC2 instance](#). Per informazioni sull'aggiornamento manuale del security agent a questa versione di release, consulta [Managing security agent manual for Amazon EC2 instance](#).

13 giugno 2024

Nuova funzionalità: protezione da malware per la disponibilità nella regione S3

GuardDuty La protezione da malware per S3 è ora disponibile in tutte le regioni commerciali in cui GuardDuty è disponibile. Questa funzionalità ti aiuta a scansionare gli oggetti appena caricati nei bucket Amazon S3 alla ricerca di potenziali malware e caricamenti sospetti e ad agire per isolarli prima che vengano inseriti nei processi downstream. [Per informazioni sull'attivazione di Malware Protection for S3, consulta Malware Protection for S3. GuardDuty](#)

12 giugno 2024

Nuova funzionalità: protezione da malware per S3

11 giugno 2024

GuardDuty annuncia la disponibilità generale di Malware Protection for S3 che ti aiuta a scansionare gli oggetti appena caricati nei bucket Amazon S3 alla ricerca di potenziali malware e caricamenti sospetti e ad agire per isolarli prima che vengano inseriti nei processi downstream. Questa funzionalità è completamente gestita da AWS GuardDuty pubblica il risultato della scansione degli oggetti S3 sul bus eventi EventBridge predefinito. È possibile consentire GuardDuty l'aggiunta di tag agli oggetti S3 scansionati. È possibile creare flussi di lavoro a valle, come l'isolamento in un bucket di quarantena, o definire politiche relative ai bucket utilizzando tag che impediscono agli utenti o alle applicazioni di accedere a determinati oggetti. [Per ulteriori informazioni, consulta GuardDuty Malware Protection for S3](#). Attualmente è disponibile nelle seguenti regioni:

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)

- Stati Uniti occidentali (Oregon)
- Europa (Irlanda)
- Europa (Francoforte)
- Europa (Stoccolma)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Asia Pacifico (Singapore)

[Policy AmazonGuardDutyFullAccess aggiornata](#)

È stata aggiunta l'autorizzazione che consente di assegnare un ruolo IAM a GuardDuty quando si attiva Malware Protection for S3. Per ulteriori informazioni su questo aggiornamento della politica, consulta la [policy AWS gestita: AmazonGuardDutyFullAccess](#).

10 giugno 2024

[Funzionalità aggiornata in GuardDuty RDS Protection](#)

RDS Protection estende il supporto per monitorare l'attività di accesso sui database RDS per PostgreSQL. Come parte di questa espansione, GuardDuty inizierà automaticamente il monitoraggio dei dati di accesso dai database RDS per PostgreSQL per gli account che hanno già abilitato la protezione RDS. GuardDuty [Per ulteriori informazioni, consulta RDS Protection](#).

6 giugno 2024

[Funzionalità aggiornata in GuardDuty Runtime Monitoring - Fargate \(solo Amazon ECS\)](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.2.0 per le risorse AWS Fargate (solo Amazon ECS). Per ulteriori informazioni sulle note di rilascio, vedere [GuardDuty Security Agent for Fargate-ECS](#).

31 maggio 2024

[Funzionalità aggiornata in GuardDuty Malware Protection for EC2](#)

Per ogni volume Amazon EBS collegato alle istanze Amazon EC2 e ai carichi di lavoro dei container GuardDuty , Malware Protection for EC2 ha aumentato le dimensioni del volume EBS sottoposti a scansione fino a 2048 GB. Per informazioni sulla scansione dei volumi Amazon EBS collegati alle tue istanze, consulta [GuardDuty Malware Protection for EC2](#).

29 maggio 2024

[Funzionalità aggiornate in Runtime Monitoring](#)

Il monitoraggio del runtime per le risorse di Amazon ECS-Fargate ora supporta il rilevamento di potenziali minacce sulle attività avviate da e. AWS Batch AWS CodePipeline Per ulteriori informazioni, consulta [Come funziona il monitoraggio del runtime con Fargate \(solo Amazon ECS\)](#).

28 maggio 2024

[Funzionalità aggiornata in Runtime Monitoring](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.6.1 per le risorse Amazon EKS. Per informazioni sulle note di rilascio, consulta la cronologia dei rilasci [dell'agente aggiuntivo EKS](#).

14 maggio 2024

[Supporto regionale esteso per il monitoraggio del runtime](#)

GuardDuty estende il supporto per Runtime Monitoring alla regione Canada occidentale (Calgary). Per informazioni su come iniziare a usare Runtime Monitoring, consulta [Enabling Runtime Monitoring](#).

7 maggio 2024

[Supporto regionale esteso per la protezione RDS](#)

GuardDuty estende il supporto di RDS Protection a quanto segue: Regioni AWS

3 maggio 2024

- Canada occidentale (Calgary)
- Asia Pacifico (Hyderabad)
- Europa (Spagna)
- Europa (Zurigo)
- Medio Oriente (Emirati Arabi Uniti)
- Israele (Tel Aviv)
- Asia Pacifico (Melbourne)

Per informazioni sull'attivazione di questa funzionalità, consulta [RDS Protection](#).

[Funzionalità aggiornata in Runtime Monitoring](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.1.0 per le risorse AWS Fargate (solo Amazon ECS). Per ulteriori informazioni sulle note di rilascio, vedere [GuardDuty Security Agent for Fargate-ECS](#).

1° maggio 2024

[Funzionalità aggiornata in Runtime Monitoring](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.6.0 per le risorse Amazon EKS. Per informazioni sulle note di rilascio, consulta la cronologia dei rilasci [dell'agente aggiuntivo EKS](#).

29 aprile 2024

[Support per IPAddresssv6](#)

GuardDuty ha aggiunto IPAddresssv6 il supporto per i dettagli IP locali e remoti. È possibile utilizzare gli [attributi Filter associati per filtrare](#) GuardDuty i risultati o [creare regole di soppressione](#).

18 aprile 2024

[Esperienza di console aggiornata per configurare l'esportazione dei risultati](#)

GuardDuty ha aggiornato l'esperienza della console per esportare i risultati generati nel tuo Account AWS bucket Amazon S3. Per ulteriori informazioni, consulta [Esportazione GuardDuty](#) dei risultati.

1 aprile 2024

[Funzionalità aggiornata in Runtime Monitoring](#)

Runtime Monitoring ha rilasciato 28 marzo 2024
o una nuova versione del security agent 1.1.0 per la risorsa Amazon EC2. Questa versione supporta la configurazione GuardDuty automatic a degli agenti in Runtime Monitoring per le istanze Amazon EC2. Per informazioni sulle note di rilascio, consulta [GuardDuty Security Agent for Amazon EC2 instance](#).

[Disponibilità generale del Runtime Monitoring per le istanze Amazon EC2](#)

28 marzo 2024

GuardDuty annuncia la disponibilità generale (GA) di Runtime Monitoring per le istanze Amazon EC2. Ora hai la possibilità di [abilitare la configurazione automatizzata dell'agente](#) che consente GuardDuty di installare e gestire l'agente di sicurezza per le tue istanze Amazon EC2 per tuo conto. Con l'agente GuardDuty automatizzato, puoi anche utilizzare tag di inclusione o esclusione e GuardDuty per informare sull'installazione e sulla gestione del security agent solo su istanze Amazon EC2 selezionate. Per ulteriori informazioni, consulta [Come funziona il monitoraggio del runtime con le istanze Amazon EC2](#).

Elenco di nuovi tipi di ricerca rilasciati insieme a questa GA

- [Esecuzione: Runtime/SuspiciousTool](#)
- [Esecuzione: Runtime/SuspiciousCommand](#)
- [DefenseEvasionEsecuzione: Runtime/ ----sep----:runtime/SuspiciousCommand](#)

- [DefenseEvasion:Runtime/ ----Sep----:Runtime/PtraceAntiDebugging](#)
- [Esecuzione: Runtime/MaliciousFileExecuted](#)

[Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi \(SLR\)](#)

26 marzo 2024

Usa AWS Systems Manager le azioni per gestire le associazioni SSM sulle istanze Amazon EC2 quando GuardDuty abilita il monitoraggio del runtime con agente automatizzato per Amazon EC2. Quando la configurazione GuardDuty automatizzata degli agenti è disabilitata, GuardDuty considera solo le istanze EC2 che hanno un tag di inclusione (:). GuardDutyManaged true

- L'elenco seguente mostra le nuove autorizzazioni:

```
"ssm:DescribeAssociation",  
"ssm:DeleteAssociation",  
"ssm:UpdateAssociations",  
"ssm:CreateAssociation",  
"ssm:StartAssociationsOnce",  
"ssm:AddTagsToResource",  
"ssm:CreateAssociation",  
"ssm:UpdateAssociation",  
"ssm:SendCommand",  
"ssm:GetCommandInvocation"
```

[Funzionalità aggiornate in Runtime Monitoring](#)

Con l'ultima versione GuardDuty di Security Agent (add-on) v1.5.0 per Amazon EKS, Runtime Monitoring ora supporta la configurazione di parametri specifici del tuo GuardDuty security agent, come impostazioni di CPU e memoria, impostazioni e impostazioni dei PriorityClass criteri DNS. Per ulteriori informazioni, consulta [Configurazione dei parametri dell'agente di GuardDuty sicurezza](#) (componente aggiuntivo EKS).

7 marzo 2024

[Funzionalità aggiornata in Runtime Monitoring](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.5.0 per le risorse Amazon EKS. Per informazioni sulle note di rilascio, consulta la cronologia dei [rilaschi dell'agente aggiuntivo EKS](#).

7 marzo 2024

[Supporto per Canada West \(Calgary\)](#)

Amazon GuardDuty è ora disponibile nella regione Canada occidentale (Calgary). Alcuni dei piani di protezione e inclusi GuardDuty potrebbero non essere disponibili in questa regione. Per le informazioni più recenti, consulta [Regioni ed endpoint](#).

6 marzo 2024

[Funzionalità aggiornata in Runtime Monitoring](#)

Le versioni GuardDuty di security agent 1.0.0 e 1.1.0 per i cluster Amazon EKS non saranno più supportate a partire dal 14 maggio 2024. Per informazioni sui passaggi da eseguire prima della fine del supporto standard, consulta l'[agente di GuardDuty sicurezza per i cluster Amazon EKS](#).

16 febbraio 2024

[Funzionalità aggiornate in Runtime Monitoring](#)

Runtime Monitoring supporta l'ultima versione di [Kubernete s 1.29 con la versione 1.4.1](#) del Security Agent esistente . Il supporto è disponibile dal lancio di questa versione di Kubernetes. Per informazioni sulle versioni di Kubernetes supportate, consulta Versioni di Kubernetes supportate dal security [agent](#). GuardDuty

16 febbraio 2024

[Funzionalità aggiornata in Runtime Monitoring - Disponibilità regionale](#)

GuardDuty II Runtime Monitoring ora supporta Amazon VPC condiviso all'interno dello stesso. AWS Organizations [GuardDuty service-linked role \(SLR\)](#) ha una nuova autorizzazione, `organizations:DescribeOrganization` che aiuta a recuperare l'ID dell'organizzazione per l'account Amazon VPC condiviso per impostare la policy degli endpoint. Per informazioni sui prerequisiti per l'utilizzo di un endpoint Amazon VPC condiviso in Runtime Monitoring, consulta [Supporto per Amazon VPC condiviso](#). Questa funzionalità è disponibile in tutte le regioni in cui GuardDuty supporta il monitoraggio del runtime.

12 febbraio 2024

[Funzionalità aggiornata in Runtime Monitoring - Disponibilità regionale](#)

GuardDuty II Runtime Monitoring ora supporta Amazon VPC condiviso all'interno dello stesso. AWS Organizations [GuardDuty service-linked role \(SLR\)](#) ha una nuova autorizzazione, `organizations:DescribeOrganization` che aiuta a recuperare l'ID dell'organizzazione per l'account Amazon VPC condiviso per impostare la policy degli endpoint. Per informazioni sui prerequisiti per l'utilizzo di un endpoint Amazon VPC condiviso in Runtime Monitoring, consulta [Supporto per Amazon VPC condiviso](#). Attualmente, questa funzionalità è disponibile in alcuni dei. Regioni AWS Per maggiori informazioni, consulta [Regioni ed endpoint di](#).

9 febbraio 2024

[Funzionalità aggiornata con supporto per la nuova funzionalità Regioni AWS : Malware Protection for EC2](#)

Malware Protection for EC2 ora supporta la scansione dei volumi EBS crittografati con Chiavi gestite da AWS nella regione Stati Uniti occidentali (Oregon).

6 febbraio 2024

[Funzionalità aggiornata con supporto per la nuova funzionalità Regioni AWS : Malware Protection for EC2](#)

[Malware Protection for EC2 ora supporta la scansione dei volumi EBS crittografati con Chiavi gestite da AWS nei seguenti modi: Regioni AWS](#)

5 febbraio 2024

- Asia Pacifico (Singapore) (ap-southeast-1)
- Europa (Francoforte) (eu-central-1)
- Asia Pacifico (Osaka-Locale) (ap-northeast-3)
- Stati Uniti orientali (Ohio) (us-east-2)
- Europa (Milano) (eu-south-1)
- Asia Pacifico (Tokyo) (ap-northeast-1)
- Asia Pacifico (Seoul) (ap-northeast-2)
- Canada (Centrale) (ca-central-1)
- Europa (Irlanda) (eu-west-1)
- Stati Uniti orientali (Virginia settentrionale) (us-east-1)

[Funzionalità aggiornate in Runtime Monitoring](#)

GuardDuty Runtime Monitoring ha rilasciato una nuova versione del GuardDuty security agent (v1.0.2) per le istanze Amazon EC2. Questa versione agente include il supporto per la versione più recente di Amazon ECS. AMIs

Per ulteriori informazioni sulla cronologia dei rilasci degli agenti, consulta [GuardDuty Security Agent for Amazon EC2 Instances](#).

2 febbraio 2024

[Funzionalità aggiornata con supporto per la nuova funzionalità Regioni AWS : Malware Protection for EC2](#)

[Malware Protection for EC2 ora supporta la scansione dei volumi Amazon EBS crittografati con Chiavi gestite da AWS nei seguenti modi: Regioni AWS](#)

31 gennaio 2024

- Europa (Londra) (eu-west-2)
- Europa (Stoccolma) (eu-north-1)
- Asia Pacifico (Hong Kong) (ap-east-1)
- Africa (Città del Capo) (af-south-1)
- Medio Oriente (Bahrein) (me-south-1)
- Asia Pacifico (Hyderabad) (ap-south-2)
- Europa (Spagna) (eu-south-2)
- Asia Pacifico (Melbourne) (ap-southeast-4)
- Asia Pacifico (Sydney) (ap-southeast-2)
- Israele (Tel Aviv) (il-central-1)

[Aggiornamento: Gestione degli account con AWS Organizations](#)

È stato riorganizzato il contenuto in [Gestione degli account con AWS Organizations](#). , ha aggiunto la procedura per modificare l'account GuardDuty amministratore delegato e aggiornato [Comprensione della relazione tra account GuardDuty amministratore e account membro](#).

30 gennaio 2024

[Funzionalità aggiornata con supporto per nuove Regioni AWS](#)

[Malware Protection for EC2](#) ora supporta la scansione dei volumi EBS crittografati con Chiavi gestite da AWS nei seguenti modi: [Regioni AWS](#)

29 gennaio 2024

- Asia Pacifico (Giacarta) (ap-southeast-3)
- Stati Uniti occidentali (California settentrionale) (us-west-1)
- Medio Oriente (EAU) (me-central-1)
- Europa (Zurigo) (eu-central-2)
- Asia Pacifico (Mumbai) (ap-south-1)
- Sud America (San Paolo) (sa-east-1)

[Funzionalità aggiornata in Malware Protection for EC2](#)

25 gennaio 2024

Malware Protection for EC2 ora supporta la scansione dei volumi EBS crittografati utilizzando. Chiavi gestite da AWS [Malware Protection for EC2 service-linked role \(SLR\)](#) ha due nuove autorizzazioni: e. GetSnapshotBlock ListSnapshotBlocks

[Queste autorizzazioni aiuteranno a GuardDuty recuperare l'istantanea di un volume EBS \(con crittografia Chiave gestita da AWS\) dall'utente Account AWS e a copiarla sull'account del servizio prima di avviare la scansione antimalware.](#) [GuardDuty](#) Attualmente, questa funzionalità è disponibile solo in Europa (Parigi) (). eu-west-3 Per ulteriori informazioni, vedere [Volumi supportati per la scansione antimalware.](#)

[Funzionalità aggiornata in Runtime Monitoring](#)

GuardDuty Runtime Monitoring ha rilasciato una nuova versione del GuardDuty Security Agent (v1.0.1) con ottimizzazione e miglioramenti generali delle prestazioni. Per ulteriori informazioni sulla cronologia dei rilasci degli agenti, consulta [GuardDuty Security Agent for Amazon EC2 Instances](#).

23 gennaio 2024

[Funzionalità aggiornate in Runtime Monitoring](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.1 per le risorse Amazon EKS. Per ulteriori informazioni, consulta [Cronologia delle versioni dell'agente \(componente aggiuntivo EKS\)](#).

16 gennaio 2024

[Runtime Monitoring ha rilasciato il nuovo agente v1.4.0 per le risorse Amazon EKS](#)

Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.0 per le risorse Amazon EKS. Per ulteriori informazioni, consulta [Cronologia delle versioni dell'agente \(componente aggiuntivo EKS\)](#).

21 dicembre 2023

[Aggiunti tipi di risultati basati su S3 e AWS CloudTrail machine learning \(ML\) in Europa \(Zurigo\), Europa \(Spagna\), Asia Pacifico \(Hyderabad\), Asia Pacifico \(Melbourne\) e Israele \(Tel Aviv\)](#)

Il seguente S3 e CloudTrail i risultati che identificano il comportamento anomalo utilizzando il modello GuardDuty di machine learning (ML) di rilevamento delle anomalie sono ora disponibili nelle regioni di Europa (Zurigo), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne) e Israele (Tel Aviv):

21 dicembre 2023

- [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 supporta 50.000 account membri tramite AWS Organizations](#)

Un GuardDuty amministratore delegato può ora gestire un massimo di 50.000 account membri tramite AWS Organizations. Ciò include anche un massimo di 5000 account membri associati all'account GuardDuty amministratore tramite invito.

20 dicembre 2023

[GuardDuty Il supporto per il monitoraggio del runtime è stato esteso a 19 Regioni AWS](#)

Runtime Monitoring è ora disponibile in Asia Pacifico (Giacarta), Europa (Parigi), Asia Pacifico (Osaka), Asia Pacifico (Seoul), Medio Oriente (Bahrein), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Israele (Tel Aviv), Stati Uniti occidentali (California settentrionale), Europa (Londra), Asia Pacifico (Hong Kong), Europa (Milano), Medio Oriente (Emirati Arabi Uniti), Sud America (San Paolo), Asia Pacifico (Mumbai), Canada (Centrale), Africa (Città del Capo), Europa (Zurigo).

6 dicembre 2023

[GuardDuty espande la funzionalità di monitoraggio del runtime](#)

Oltre a rilevare le minacce ai cluster Amazon EKS, GuardDuty annuncia la disponibilità generale di Runtime Monitoring per rilevare le minacce ai carichi di lavoro Amazon ECS e una versione di anteprima per rilevare le minacce alle istanze Amazon EC2. [Per ulteriori informazioni su quali Regioni AWS attualmente supportano il Runtime Monitoring, consulta Regioni ed endpoint.](#)

26 novembre 2023

[Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi \(SLR\)](#)

GuardDuty ha aggiunto nuove autorizzazioni per utilizzare le azioni Amazon ECS per gestire e recuperare informazioni sui cluster Amazon ECS e gestire le impostazioni dell'account Amazon ECS con `guarddutyActivate`. Le azioni relative ad Amazon ECS recuperano anche le informazioni sui tag associati a GuardDuty.

26 novembre 2023

- [Le seguenti autorizzazioni sono state aggiunte come parte dell'espansione della funzionalità di monitoraggio del runtime:](#)

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

[Sono state aggiornate le politiche AWS gestite](#)

GuardDuty ha aggiunto una nuova autorizzazione, `organizations:ListAccounts` alla [politica AWS gestita: AmazonGuardDutyFullAccess](#) e [AmazonGuardDutyReadOnlyAccess](#).

16 novembre 2023

[GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.](#)

11 novembre 2023

EKS Audit Log Monitoring ora supporta i seguenti tipi di risultati in Asia Pacifico (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

[GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.](#)

10 novembre 2023

EKS Audit Log Monitoring ora supporta i seguenti tipi di ricerca nelle regioni Asia Pacifico (Hyderabad-south-2), Europa (Zurigoeu-central-2) ed Europa (Spagna) (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 ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.](#)

8 novembre 2023

EKS Audit Log Monitoring ora supporta i seguenti tipi di risultati. Questi tipi di risultati non sono ancora disponibili nelle regioni Asia Pacifico (Hyderabadap-south-2) (), Europa (Zurigo) (eu-central-2), Europa (Spagna) (eu-south-2) e Asia Pacifico (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

[Il monitoraggio del runtime EKS ha rilasciato il nuovo agente v1.3.1](#)

EKS Runtime Monitoring ha rilasciato una nuova versione 1.3.1 dell'agente che include importanti patch e aggiornamenti di sicurezza.

23 ottobre 2023

[Nuovo attributo del filtro per gli esiti](#)

GuardDuty ha aggiunto nuovi criteri per filtrare i risultati generati. Il suffisso del dominio di richiesta DNS fornisce il dominio di secondo e primo livello coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.

17 ottobre 2023

[Il monitoraggio del runtime EKS ha rilasciato il nuovo agente v1.3.0 che supporta la versione 1.28 di Kubernetes](#)

EKS Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 che supporta la versione 1.28 di Kubernetes. È stato aggiunto il supporto per Ubuntu. Per ulteriori informazioni, consulta [Cronologia delle versioni dell'agente \(componente aggiuntivo EKS\)](#).

5 ottobre 2023

[Aggiunti tipi di risultati basati su S3 e AWS CloudTrail machine learning \(ML\) alle regioni Asia Pacifico \(Giacarta\) e Medio Oriente \(Emirati Arabi Uniti\)](#)

20 settembre 2023

Le seguenti informazioni su S3 e CloudTrail i risultati che identificano il comportamento anomalo utilizzando il modello GuardDuty di apprendimento automatico per il rilevamento delle anomalie (ML) sono ora disponibili nelle regioni di Asia Pacifico (Giacarta) e Medio Oriente (Emirati Arabi Uniti):

- [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 introduce la gestione dell'agente di sicurezza a livello di cluster GuardDuty](#)

EKS Runtime Monitoring aggiunge il supporto per la gestione dell'agente di GuardDuty sicurezza per i singoli cluster EKS per monitorare gli eventi di runtime solo da questi cluster selettivi . Il monitoraggio del runtime EKS estende questa funzionalità aggiungendo il supporto di tag.

13 settembre 2023

[GuardDuty Malware Protection for EC2 estende il supporto a molti altri Regioni AWS](#)

La protezione da malware per EC2 è ora disponibile in Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Europa (Zurigo) ed Europa (Spagna).

11 settembre 2023

[GuardDuty è ora disponibile nella regione di Israele \(Tel Aviv\)](#)

È stata aggiunta la regione di Israele (Tel Aviv) all'elenco Regioni AWS dei paesi GuardDuty in cui è ora disponibile. I seguenti piani di protezione sono disponibili anche nella regione Israele (Tel Aviv):

24 agosto 2023

- [Protezione EKS](#) include il monitoraggio dei log di audit EKS e il monitoraggio del runtime EKS.
- [Protezione Lambda](#).
- [Protezione da malware per EC2](#).
- [Protezione S3](#).

Per ulteriori informazioni sulla disponibilità del piano di protezione nella regione Israele (Tel Aviv), consulta [Regioni ed endpoint](#).

[GuardDuty aggiunta della configurazione di attivazione automatica per l'organizzazione a livello di piano di protezione](#)

Aggiorna la configurazione dell'organizzazione per i piani di protezione nella tua regione. Le opzioni di configurazione possibili sono: abilitazione per tutti gli account, abilitazione automatica per i nuovi account o abilitazione automatica disattivata per tutti gli account dell'organizzazione.

16 agosto 2023

[I tipi di ricerca S3 che identificano comportamenti anomali utilizzando il modello GuardDuty di machine learning \(ML\) per il rilevamento delle anomalie sono ora disponibili in Asia Pacifico \(Osaka\)](#)

I seguenti tipi di esiti sono ora disponibili nella regione Asia Pacifico (Osaka-Locale):

10 agosto 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[Il monitoraggio del runtime EKS è ora disponibile in Asia Pacifico \(Melbourne\)](#)

EKS Runtime Monitoring all'interno di GuardDuty EKS Protection fornisce il rilevamento delle minacce di runtime per i cluster Amazon EKS nell'AWS ambiente. Ora è disponibile nella regione Asia Pacifico (Melbourne).

8 agosto 2023

[È stato aggiornato l'elenco dei GuardDuty risultati che richiamano la scansione antimalware GuardDuty avviata](#)

Alcuni tipi di risultati di EKS Runtime Monitoring possono ora richiamare la scansione GuardDuty antimalware avviata nel tuo Account AWS

19 luglio 2023

[GuardDuty supporta 10.000 account membri tramite AWS Organizations](#)

Un account GuardDuty amministratore può ora gestire un massimo di 10.000 account membri tramite AWS Organizations. Ciò include anche un massimo di 5000 account membri associati all'account GuardDuty amministratore su invito.

29 giugno 2023

[Il monitoraggio del runtime EKS annuncia tre nuovi tipi di esiti.](#)

Il monitoraggio del runtime EKS supporta tre nuovi tipi di esiti basati sulla tecnica di iniezione del processo. I nuovi tipi di ricerca sono DefenseEvasion:Runtime/ProcessInjection.Proc, DefenseEvasion:Runtime/ProcessInjection.Ptrace, and DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.

22 giugno 2023

[Il monitoraggio del runtime EKS ha rilasciato il nuovo agente v1.2.0 che supporta la versione 1.27 di Kubernetes](#)

EKS Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.2.0 che supporta anche le istanze ARM64 basate. È stato aggiunto il supporto per Bottlerocket. Per ulteriori informazioni, consulta [Cronologia delle versioni dell'agente \(componente aggiuntivo EKS\)](#).

16 giugno 2023

[GuardDuty la console fornisce una visualizzazione riepilogativa dei risultati.](#)

La dashboard di riepilogo nella GuardDuty console fornisce una visualizzazione aggregata dei GuardDuty risultati. Attualmente, la dashboard mostra i dati tramite vari widget per gli ultimi 10.000 risultati generati per il tuo account (o per gli account membro se sei un account GuardDuty amministratore) per la regione corrente.

12 giugno 2023

[Il monitoraggio dei log di audit EKS è ora disponibile in Asia Pacifico \(Hyderabad\), Asia Pacifico \(Melbourne\), Europa \(Zurigo\) ed Europa \(Spagna\)](#)

Abilita EKS Audit Log Monitoring (in EKS Protection) per i tuoi account per monitorare i log di audit EKS dai tuoi cluster Amazon EKS e analizzarli per attività potenzialmente dannose e sospette.

1 giugno 2023

[Il monitoraggio dei log di audit EKS è ora disponibile in Medio Oriente \(EAU\)](#)

EKS Audit Log Monitoring è ora disponibile in Medio Oriente (Emirati Arabi Uniti). Abilita EKS Audit Log Monitoring per i tuoi account per monitorare i log di audit EKS dai tuoi cluster Amazon EKS e analizzarli per attività potenzialmente dannose e sospette.

3 maggio 2023

[GuardDuty Malware Protection for EC2 annuncia la scansione antimalware su richiesta](#)

27 aprile 2023

Malware Protection for EC2 ti aiuta a rilevare la potenziale presenza di malware nei volumi Amazon EBS collegati alle istanze Amazon EC2 e ai carichi di lavoro dei container. Ora offre due tipi di scansioni: avviate e su richiesta. GuardDuty GuardDuty-initiated malware scan avvia automaticamente una scansione senza agente nei volumi Amazon EBS solo quando GuardDuty genera uno dei Findings che richiamano la scansione antimalware avviata dall'utente. [GuardDuty](#) Puoi avviare una scansione antimalware on demand per le istanze Amazon EC2 nel tuo account fornendo il nome della risorsa Amazon (ARN) associato all'istanza Amazon EC2 in questione. [Per ulteriori informazioni sulle differenze tra i due tipi di scansione, consulta Malware Protection for EC2.](#)

- [GuardDuty-scansione antimalware avviata](#)
- [Scansione antimalware on demand](#)

[GuardDuty annuncia Lambda Protection](#)

La Protezione Lambda è utile per identificare potenziali minacce alla sicurezza nelle tue funzioni AWS Lambda .

20 aprile 2023

- [Tipi di esiti della Protezione Lambda](#)
- [Correzione di una funzione Lambda potenzialmente compromessa](#)

[GuardDuty è ora disponibile nella regione Asia Pacifico \(Melbourne\)](#)

È stata aggiunta l'area Asia Pacifico (Melbourne) all'elenco delle aree Regioni AWS in cui GuardDuty è disponibile. Per informazioni sulle funzionalità disponibili in questa regione, consulta [Regioni ed endpoint](#).

19 aprile 2023

[GuardDuty sono stati aggiunti 3 nuovi tipi di risultati EC2](#)

GuardDuty introduce nuovi tipi di ricerca per rilevare l'uso di resolver DNS esterni e tecnologie DNS crittografate. [Per informazioni su Regioni AWS dove sono supportati questi tipi di ricerca, consulta Regioni ed endpoint](#).

5 aprile 2023

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

[GuardDuty annuncia EKS Runtime Monitoring in EKS Protection](#)

30 marzo 2023

EKS Runtime Monitoring all'interno di EKS Protection fornisce il rilevamento delle minacce di runtime per i cluster Amazon EKS nell' AWS ambiente. Viene utilizzato un agente (componente aggiuntivo di Amazon EKS, `aws-guardduty-agent`) che raccoglie gli [Eventi di runtime](#) dai carichi di lavoro EKS. Dopo aver GuardDuty ricevuto questi eventi di runtime, li monitora e li analizza per identificare potenziali minacce sospette alla sicurezza. Per ulteriori informazioni, consulta [Dettagli sui risultati](#) e [Tipi di esiti del monitoraggio del runtime EKS](#).

[GuardDuty aggiunge
una nuova funzionalità:
autoEnableOrganizationMembers](#)

Amazon GuardDuty aggiunge una nuova opzione di configurazione dell'organizzazione che aiuta a controllare e applicare gli account degli GuardDuty amministratori (se necessari o) GuardDuty abilitata per ALL i membri dell'organizzazione. La best practice consiste ora nell'utilizzare `autoEnableOrganizationMembers` invece di `autoEnable`. L'opzione `autoEnable` è obsoleta, ma è ancora supportata. Quanto segue è APIs interessato da questa nuova funzionalità:

23 marzo 2023

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[La funzionalità RDS Protection in Amazon GuardDuty è ora disponibile a livello generale](#)

GuardDuty RDS Protection monitora e profila l'attività di accesso RDS per identificare comportamenti di accesso sospetti sulle istanze del database Amazon Aurora. Per informazioni sulle Regioni AWS che supportano la Protezione RDS, consulta [Regioni ed endpoint](#).

16 marzo 2023

[GuardDuty annuncia l'attivazione della funzionalità](#)

In passato, l' GuardDuty API consentiva la configurazione sia delle funzionalità che delle fonti di dati, ma ora tutti i nuovi tipi di GuardDuty protezione e verranno configurati come funzionalità e non come fonti di dati. GuardDuty supporta ancora le fonti di dati tramite API ma non aggiungerà una nuova API. L'attivazione delle funzionalità influisce sul comportamento dell'utente APIs che abilita GuardDuty o su un tipo di protezione interno GuardDuty. Se gestisci i tuoi GuardDuty account tramite API, SDK o modello CFN, consulta le [modifiche all'Guard Duty API di marzo 2023](#).

16 marzo 2023

[GuardDuty Malware Protection for EC2 è ora disponibile nella regione del Medio Oriente \(Emirati Arabi Uniti\)](#)

La funzionalità Malware Protection for EC2 GuardDuty è supportata nella regione del Medio Oriente (Emirati Arabi Uniti). Per maggiori informazioni, consulta [Regioni ed endpoint di](#).

13 marzo 2023

[Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi \(SLR\)](#)

GuardDuty ha aggiunto le seguenti nuove autorizzazioni per supportare la prossima funzionalità GuardDuty EKS Runtime Monitoring.

8 marzo 2023

- Utilizza le operazioni di Amazon EKS per gestire e recuperare informazioni sui cluster EKS e gestisci i componenti aggiuntivi EKS su questi cluster. Le azioni EKS recuperano anche le informazioni sui tag associati a GuardDuty

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"ec2:DescribeVpcEndpointServices",  
"ec2:DescribeSecurityGroups"
```

Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi (SLR)	La GuardDuty SLR è stata aggiornata per consentire la creazione di Malware Protection for EC2 SLR dopo l'attivazione di Malware Protection for EC2.	21 febbraio 2023
GuardDuty richiede TLS v1.2 o versione successiva	Per comunicare con AWS le risorse, GuardDuty richiede e supporta TLS v1.2 o versione successiva. Per ulteriori informazioni, consulta Protezione dei dati e Sicurezza dell'infrastruttura .	14 febbraio 2023
GuardDuty è ora disponibile nella regione Asia Pacifico (Hyderabad)	È stata aggiunta la regione Asia Pacifico (Hyderabad) all'elenco delle Regioni AWS aree in cui è disponibile. GuardDuty Per maggiori informazioni, consulta Regioni ed endpoint di .	14 febbraio 2023
Amazon GuardDuty User Guide è in linea con le best practice IAM	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM .	10 febbraio 2023
GuardDuty è ora disponibile nella regione Europa (Spagna)	È stata aggiunta Europa (Spagna) all'elenco Regioni AWS dei paesi GuardDuty in cui è disponibile. Per maggiori informazioni, consulta Regioni ed endpoint di .	8 febbraio 2023

[GuardDuty è ora disponibile nella regione Europa \(Zurigo\)](#)

È stata aggiunta Europa (Zurigo) all'elenco dei paesi Regioni AWS in cui GuardDuty è disponibile. Per maggiori informazioni, consulta [Regioni ed endpoint di](#).

12 dicembre 2022

[Versione di anteprima di una nuova funzionalità: GuardDuty RDS Protection](#)

GuardDuty RDS Protection monitora e profila l'attività di accesso RDS per identificare comportamenti di accesso sospetti sulle istanze del database Amazon Aurora. Attualmente, è disponibile per una versione di anteprima in cinque Regioni AWS. Per maggiori informazioni, consulta [Regioni ed endpoint di](#).

30 novembre 2022

[GuardDuty è ora disponibile nella regione del Medio Oriente \(Emirati Arabi Uniti\)](#)

È stato aggiunto il Medio Oriente (Emirati Arabi Uniti) all'elenco delle aree Regioni AWS in cui GuardDuty è disponibile. Per maggiori informazioni, consulta [Regioni ed endpoint di](#).

6 ottobre 2022

[Contenuto aggiunto per una nuova funzionalità: GuardDuty Malware Protection for EC2](#)

GuardDuty Malware Protection for EC2 è un miglioramento opzionale di Amazon. GuardDuty Oltre a GuardDuty identificare le risorse a rischio, Malware Protection for EC2 rileva il malware che potrebbe essere all'origine della compromissione. Con Malware Protection for EC2 abilitata, ogni volta che GuardDuty rileva un comportamento sospetto su un'istanza Amazon EC2 o un carico di lavoro di container indicativo di GuardDuty malware, Malware Protection for EC2 avvia una scansione senza agente sui volumi EBS collegati all'istanza o ai carichi di lavoro dei container EC2 interessati per rilevare la presenza di malware. [Per informazioni sul funzionamento di Malware Protection for EC2 e sulla configurazione di questa funzionalità, consulta Malware Protection for EC2. GuardDuty](#)

26 luglio 2022

- [Per informazioni sui risultati di Malware Protection for EC2, consulta Finding details.](#)
- Per informazioni sulla riparazione dell'istanza

EC2 compromessa e di un contenitore autonomo, consulta [Risolvere](#) i problemi di sicurezza rilevati da GuardDuty

- [Per informazioni sul controllo dei CloudWatch log per le scansioni antimalware e sui motivi per cui una risorsa viene ignorata durante la scansione antimalware, consulta Comprendere i log e ignorare i motivi. CloudWatch](#)
- Per informazioni sui rilevamenti di minacce false positive, consulta [Segnalazione dei falsi positivi in Malware Protection for EC2](#). GuardDuty

[È stato ritirato un tipo di esito](#)

[Exfiltration:S3/ObjectRead.Unusual](#) è stato ritirato.

5 luglio 2022

[GuardDuty](#) Sono stati aggiunti nuovi tipi di ricerca S3 che identificano i comportamenti anomali utilizzando il modello di machine learning (ML) per il rilevamento delle anomalie.

Sono stati aggiunti i nuovi tipi di esiti S3 seguenti. Questi tipi di esiti rilevano se una richiesta API ha richiamato un'entità IAM in modo anomalo. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Per ulteriori informazioni su ciascuno di questi nuovi esiti, consulta [Tipi di esiti S3](#).

5 luglio 2022

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[Aggiunti contenuti GuardDuty di protezione EKS per GuardDuty](#)

GuardDuty ora puoi generare risultati per le tue risorse Amazon EKS attraverso il monitoraggio dei log di audit EKS. Per informazioni su come configurare questa funzionalità, consulta [EKS Protection in Amazon GuardDuty](#). Per un elenco dei risultati che è GuardDuty possibile generare per le risorse di Amazon EKS, consulta i risultati di [Kubernetes](#). Sono state aggiunte nuove linee guida sulla correzione e di questi esiti nella [Guida alla correzione degli esiti di Kubernetes](#).

25 gennaio 2022

[È stato aggiunto un nuovo esito](#)

È stato aggiunto un nuovo esito UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Questo risultato ti informa quando un account esterno al tuo ambiente accede alle credenziali dell'istanza. AWS AWS

20 gennaio 2022

[Sono stati aggiornati i tipi di esiti utili per identificare i problemi relativi a log4j](#)

Amazon GuardDuty ha aggiornato i seguenti tipi di risultati per aiutare a identificare e dare priorità ai problemi relativi a CVE-2021-44228 e CVE-2021-45046;;;.
Backdoor:EC2/C&CActivity.B
Backdoor:EC2/C&CActivity.B!
DNS Behavior:EC2/Netwo
rkPortUnusual

22 dicembre 2021

[Modifiche agli esiti](#)

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration è stato modificato in UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Questa versione migliorata dell'esito rileva le posizioni da cui vengono solitamente utilizzate le credenziali, riducendo così gli esiti del traffico instradato attraverso le reti on-premise.
[UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)

7 settembre 2021

[GuardDuty Aggiornamento a SLR](#)

La GuardDuty reflex è stata aggiornata con nuove azioni per migliorare la precisione di ricerca.

3 agosto 2021

[Sono state aggiunte informazioni sull'origine dati per ogni tipo di esito.](#)

Le descrizioni dei risultati ora contengono informazioni sulle fonti di dati GuardDuty utilizzati e per generare tali risultati.

10 maggio 2021

Sono stati ritirati 13 tipi di esiti.

13 risultati sono stati ritirati per essere sostituiti con nuovi AnomalousBehaviour risultati. [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](#), e [UnauthorizedAccess:IAMUser/ConsoleLogin](#).

12 marzo 2021

[Sono stati aggiunti 8 nuovi tipi di esiti per comportamenti anomali.](#)

Sono stati aggiunti 8 nuovi tipi di esiti IAMUser basati sul comportamento anomalo per i principali IAM. [CredentialAccess:IAMUser/AnomalousBehavior](#), [DefenseEvasion:IAMUser/AnomalousBehavior](#), [Discovery:IAMUser/AnomalousBehavior](#), [Exfiltration:IAMUser/AnomalousBehavior](#), [Impact:IAMUser/AnomalousBehavior](#), [InitialAccess:IAMUser/AnomalousBehavior](#), [Persistence:IAMUser/AnomalousBehavior](#), [PrivilegeEscalation:IAMUser/AnomalousBehavior](#).

12 marzo 2021

[Sono stati aggiunti alcuni esiti EC2 basati sulla reputazione del dominio.](#)

Sono stati aggiunti 4 nuovi tipi di esiti Impatto basati sulla reputazione del dominio. [Impact:EC2/AbusedDomainRequest.Reputation](#), [Impact:EC2/BitcoinDomainRequest.Reputation](#), [Impact:EC2/MaliciousDomainRequest.Reputation](#). È stata inoltre aggiunta una nuova scoperta EC2 per CActivity C&. [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

27 gennaio 2021

Sono stati aggiunti 4 nuovi tipi di esiti.	Aggiunti 3 nuovi IPCaller rilevamenti relativi a S3 Malicious. Discovery:S3/MaliciousIPCaller , Exfiltration:S3/MaliciousIPCaller . Impact:S3/MaliciousIPCaller È stata inoltre aggiunta una nuova scoperta EC2 per CActivity C&. Backdoor:EC2/C&CActivity.B	21 dicembre 2020
È stato ritirato il tipo di esito UnauthorizedAccess:EC2/TorIPCaller.	Il tipo di UnauthorizedAccess :EC2/TorIPCaller ricerca è ora GuardDuty ritirato. Ulteriori informazioni.	1° ottobre 2020
È stato aggiunto il tipo di esito Impact:EC2/WinRmBruteForce.	È stato aggiunto un nuovo esito Impatto, ossia Impact:EC2/WinRmBruteForce. Ulteriori informazioni.	17 settembre 2020
È stato aggiunto il tipo di esito Impact:EC2/PortSweep.	È stato aggiunto un nuovo esito Impatto, ossia Impact:EC2/PortSweep. Ulteriori informazioni.	17 settembre 2020
GuardDuty è ora disponibile nelle regioni Africa (Città del Capo) ed Europa (Milano).	Aggiunte Africa (Città del Capo) ed Europa (Milano) all'elenco delle AWS regioni in cui GuardDuty è disponibile. Ulteriori informazioni	31 luglio 2020

[Sono stati aggiunti nuovi dettagli di utilizzo per il monitoraggio GuardDuty dei costi.](#)

Ora puoi utilizzare nuove metriche per interrogare i dati sui costi di GuardDuty utilizzo per il tuo account e gli account che gestisci. Una nuova panoramica dei costi di utilizzo è disponibile nella console all'indirizzo <https://console.aws.amazon.com/guardduty/>. È possibile accedere a informazioni più dettagliate tramite l'API.

31 luglio 2020

[Contenuto aggiunto che copre la protezione di S3 tramite il monitoraggio degli eventi dei dati di S3 in. GuardDuty](#)

GuardDuty S3 Protection è ora disponibile tramite il monitoraggio degli eventi del piano dati S3 come nuova fonte di dati. Questa funzionalità sarà abilitata automaticamente per i nuovi account. Se lo stai già utilizzando, GuardDuty puoi abilitare la nuova fonte di dati per te o per i tuoi account membro.

31 luglio 2020

[Sono stati aggiunti 14 nuovi esiti S3.](#)

Sono stati aggiunti 14 nuovi tipi di esiti S3 per le origini del piano di controllo (control-plane) e del piano dati S3.

31 luglio 2020

[È stato aggiunto il supporto per gli esiti S3 e sono stati modificati i nomi di 2 tipi di esiti esistenti.](#)

GuardDuty i risultati ora includono maggiori dettagli sui risultati che coinvolgono i bucket S3. I tipi di esiti esistenti correlati all'attività di S3 sono stati rinominati: Policy:IAMUser/S3BlockPublicAccessDisabled è stato modificato in Policy:S3/BucketBlockPublicAccessDisabled e Stealth:IAMUser/S3ServerAccessLoggingDisabled è stato modificato in Stealth:S3/ServerAccessLoggingDisabled.

28 maggio 2020

[Contenuti aggiunti per l'integrazione AWS Organizations .](#)

GuardDuty ora si integra con gli amministratori AWS Organizations delegati per consentirti di gestire gli GuardDuty account all'interno della tua organizzazione. Quando imposti un amministratore delegato come account GuardDuty amministratore, puoi abilitare automaticamente la gestione GuardDuty di qualsiasi membro dell'organizzazione da parte dell'account amministratore delegato. Puoi anche abilitare automaticamente gli account GuardDuty dei nuovi AWS Organizations membri. [Ulteriori informazioni.](#)

20 aprile 2020

Sono stati aggiunti contenuti per la funzionalità di esportazione degli esiti.	È stato aggiunto un contenuto che descrive la funzionalità Export Findings di GuardDuty.	14 novembre 2019
È stato aggiunto il tipo di esito UnauthorizedAccess:EC2/MetadataDNSRebind.	È stato aggiunto un nuovo esito Non autorizzato, ossia UnauthorizedAccess:EC2/MetadataDNSRebind. Ulteriori informazioni.	10 ottobre 2019
È stato aggiunto il tipo di esito Stealth:IAMUser/S3ServerAccessLoggingDisabled.	È stato aggiunto un nuovo esito Stealth, ossia Stealth:IAMUser/S3ServerAccessLoggingDisabled. Ulteriori informazioni.	10 ottobre 2019
È stato aggiunto il tipo di esito Policy:IAMUser/S3BlockPublicAccessDisabled.	È stato aggiunto un nuovo esito Policy, ossia Policy:IAMUser/S3BlockPublicAccessDisabled. Ulteriori informazioni.	10 ottobre 2019
È stato ritirato il tipo di esito Backdoor:EC2/XORDDOS.	Il tipo di Backdoor:EC2/XORDDOS risultato è stato ora ritirato da GuardDuty. Scopri di più	12 giugno 2019
È stato aggiunto il tipo di esito PrivilegeEscalation.	Il tipo di esito Privilege Escalation rileva quando gli utenti tentano di assegnare privilegi di escalation più permissivi ai loro account. Ulteriori informazioni	14 maggio 2019

GuardDuty è ora disponibile nella regione Europa (Stoccolma).	È stato aggiunto Europa (Stoccolma) all'elenco delle AWS regioni in cui GuardDuty è disponibile. Ulteriori informazioni	9 maggio 2019
È stato aggiunto un nuovo tipo di esito, ossia Recon:EC2/PortProbeEMRUnprotectedPort.	Questo risultato segnala che una porta sensibile correlata a EMR su un'istanza EC2 non è bloccata ed è sottoposta attivamente a probing. Ulteriori informazioni	8 maggio 2019
Sono stati aggiunti 5 nuovi tipi di esiti in grado di rilevare se le istanze EC2 vengono potenzialmente utilizzate per attacchi Denial of Service (DoS).	Questi risultati ti informano delle istanze EC2 nell'ambiente che si comportano in un modo che potrebbe indicare che vengono utilizzate per eseguire attacchi Denial of Service (DoS). Ulteriori informazioni	8 marzo 2019
È stato aggiunto un nuovo tipo di esito: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsage type informa l'utente che le credenziali di accesso dell'utente root Account AWS vengono utilizzate per effettuare richieste programmatiche ai servizi. AWS Ulteriori informazioni	24 gennaio 2019

[Il tipo di esito UnauthorizedAccess:IAMUser/UnusualASNCaller è stato ritirato](#)

Il tipo di esito UnauthorizedAccess:IAMUser/UnusualASNCaller è stato ritirato. Ora riceverete una notifica sulle attività richiamate da reti insolite tramite altri tipi di ricerca attivi. GuardDuty Il tipo di ricerca generato sarà basato sulla categoria dell'API che è stata richiamata da una rete insolita. [Ulteriori informazioni](#)

21 dicembre 2018

[Sono stati aggiunti due nuovi tipi di esiti: PenTest:IAMUser/ParrotLinux e PenTest:IAMUser/PentooLinux](#)

I tipi di esiti PenTest:IAMUser/ParrotLinux segnalano che un computer su cui è in esecuzione e Parrot Security Linux effettua chiamate API utilizzando credenziali che appartengono al tuo account AWS . I tipi di esiti PenTest:IAMUser/PentooLinux segnalano che una macchina su cui è in esecuzione Pentoo Linux effettua chiamate API utilizzando credenziali che appartengono al tuo account AWS . [Ulteriori informazioni](#)

21 dicembre 2018

[È stato aggiunto il supporto per l'argomento GuardDuty SNS degli annunci di Amazon](#)

Ora puoi iscriverti all'argomento « GuardDuty Annunci» su SNS per ricevere notifiche sui nuovi tipi di risultati rilasciati, aggiornamenti ai tipi di risultati esistenti e altre modifiche alle funzionalità. Le notifiche sono disponibili in tutti i formati supportati da Amazon SNS.

[Ulteriori informazioni](#)

21 novembre 2018

[Sono stati aggiunti due nuovi tipi di esiti: UnauthorizedAccess:EC2/TorClient e UnauthorizedAccess:EC2/TorRelay](#)

UnauthorizedAccess:EC2/TorClientfinding type ti informa che un'istanza EC2 nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority . UnauthorizedAccess:EC2/TorRelayfinding type ti informa che un'istanza EC2 nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor.

[Ulteriori informazioni](#)

16 novembre 2018

[È stato aggiunto un nuovo tipo di esito: Cryptocurrency:EC2/BitcoinTool.B](#)

Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente sta interrogando un nome di dominio associato a Bitcoin o ad altre attività legate alle criptovalute. [Ulteriori informazioni](#)

9 novembre 2018

[È stato aggiunto il supporto per l'aggiornamento della frequenza delle notifiche inviate a Events CloudWatch](#)

Ora puoi aggiornare la frequenza delle notifiche inviate a CloudWatch Events per le successive occorrenze di risultati esistenti. I valori possibili sono 15 minuti, 1 ora o 6 ore (impostazione predefinita). [Ulteriori informazioni](#)

9 ottobre 2018

[È stato aggiunto il supporto per una regione](#)

[È stato aggiunto il supporto regionale per AWS GovCloud \(Stati Uniti occidentali\)](#) [Ulteriori informazioni](#)

25 luglio 2018

[È stato aggiunto il supporto per in CloudFormation StackSets GuardDuty](#)

Puoi utilizzare il GuardDuty modello Enable Amazon per eseguire l'attivazione GuardDuty simultanea in più account. [Ulteriori informazioni](#)

25 giugno 2018

[Aggiunto il supporto per le regole di GuardDuty archiviazione automatica](#)

I clienti possono ora creare regole di archiviazione automatica granulari per la soppressione dei risultati. I risultati che corrispondono a una regola di archiviazione automatica, li contrassegna GuardDuty automaticamente come archiviati. Ciò consente ai clienti di effettuare ulteriori ottimizzazioni GuardDuty per conservare solo i risultati pertinenti nella tabella dei risultati corrente. [Ulteriori informazioni](#)

4 maggio 2018

[GuardDuty è disponibile nella regione Europa \(Parigi\)](#)

GuardDuty è ora disponibile in Europa (Parigi) e consente di estendere il monitoraggio continuo della sicurezza e il rilevamento delle minacce in questa regione. [Ulteriori informazioni](#)

29 marzo 2018

[CloudFormation È ora supportata la creazione di account GuardDuty amministratore e account membro tramite.](#)

Per ulteriori informazioni, consultare [AWS::GuardDuty::master](#) e [AWS::GuardDuty::member](#).

6 marzo 2018

[Sono stati aggiunti nove nuovi rilevamenti di anomalie CloudTrail basati.](#)

Questi nuovi tipi di ricerca vengono abilitati automaticamente GuardDuty in tutte le regioni supportate. [Ulteriori informazioni](#)

28 febbraio 2018

[Aggiunti tre nuovi rilevamenti di intelligence sulle minacce \(individuazione dei tipi\).](#)

Questi nuovi tipi di ricerca vengono abilitati automaticamente GuardDuty in tutte le regioni supportate. [Ulteriori informazioni](#)

5 febbraio 2018

[Aumento del limite per GuardDuty gli account dei membri.](#)

Con questa versione, è possibile aggiungere fino a 1000 account GuardDuty membro per AWS account (account GuardDuty amministratore). [Ulteriori informazioni](#)

25 gennaio 2018

[Modifiche al caricamento e ulteriore gestione degli elenchi di IP affidabili e degli elenchi di minacce per gli account GuardDuty amministratore e gli account dei membri.](#)

Con questa versione, gli utenti degli GuardDuty account amministratore possono caricare e gestire elenchi di IP affidabili ed elenchi di minacce. Gli utenti degli GuardDuty account membri non possono caricare e gestire elenchi. Gli elenchi di IP affidabili e gli elenchi di minacce caricati dall'account amministratore non possono GuardDuty funzionare e correttamente negli account dei membri. [Ulteriori informazioni](#)

25 gennaio 2018

Aggiornamenti precedenti

Modifica	Descrizione	Data
Pubblicazione iniziale	Pubblicazione iniziale della Amazon GuardDuty User Guide.	28 novembre 2017

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.