



Guía del usuario de Amazon GuardDuty

Amazon GuardDuty



Amazon GuardDuty: Guía del usuario de Amazon GuardDuty

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es GuardDuty?	1
Características de GuardDuty	2
Conformidad con DSS de PCI	6
Precios en GuardDuty	6
Utilizar la prueba gratuita de 30 días de GuardDuty	7
Utilizar la protección contra malware para S3 con el nivel gratuito de 12 meses	9
Acceso a GuardDuty	9
Conceptos y términos clave	11
Introducción	17
Antes de empezar	17
Paso 1: habilitación de Amazon GuardDuty	19
Paso 2: generación de resultados de muestra y exploración de las operaciones básicas	21
Paso 3: configuración de la exportación de los resultados de GuardDuty a un bucket de Amazon S3	23
Paso 4: configuración de alertas de resultados de GuardDuty a través de SNS	28
Pasos a seguir a continuación	31
Orígenes de datos fundamentales	33
Eventos de administración de AWS CloudTrail	33
Cómo administra GuardDuty los eventos globales de AWS CloudTrail	34
Logs de flujo de VPC	35
Registros de consultas de DNS de Route53 Resolver	36
Detección Extendida de Amenazas	37
Ejemplos de escenarios de amenazas en la secuencia de ataque	37
Cómo funciona la Detección Extendida de Amenazas	38
Habilitar planes de protección para maximizar la detección de amenazas	39
Detección de secuencias de ataque en clústeres de Amazon EKS	40
Detección de secuencias de ataques en los buckets de Amazon S3	41
Detección extendida de amenazas en la consola de GuardDuty	41
Descripción y administración de resultados de secuencias de ataques	42
Recursos adicionales	42
EKS Protection	44
Registros de auditoría de EKS en EKS Protection	45
Habilitar EKS Protection en entornos de varias cuentas	45
Habilitar EKS Protection para una cuenta independiente	53

Protección de S3	55
Eventos de datos de AWS CloudTrail para S3	56
Cómo GuardDuty utiliza los eventos de datos de CloudTrail para S3	56
GuardDuty utiliza los eventos de datos de CloudTrail para S3 para las secuencias de ataque	57
Habilitar la protección de S3 en entornos de varias cuentas	57
Habilitar la S3 Protection para una cuenta independiente	64
Supervisión en tiempo de ejecución	67
Funcionamiento	68
Con clústeres de Amazon EKS	70
Con instancias de Amazon EC2	75
Con Fargate (solo Amazon ECS)	78
Después de habilitar la supervisión en tiempo de ejecución	81
Prueba gratuita de 30 días	83
Utilizo el periodo de prueba de GuardDuty o nunca he habilitado la supervisión en tiempo de ejecución de EKS	83
Habilité la supervisión en tiempo de ejecución de EKS antes del lanzamiento de la supervisión en tiempo de ejecución	84
Requisitos previos	85
Para la instancia de EC2	85
Para el clúster de Fargate (solo ECS)	91
Para el clúster de EKS	97
Habilitación de la supervisión en tiempo de ejecución	101
Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas	102
Habilitar la Supervisión en tiempo de ejecución para una cuenta independiente	107
Administrar los agentes de seguridad de GuardDuty	108
Agente automatizado en el recurso de Amazon EC2	108
Administración manual del agente para el recurso de Amazon EC2	122
Agente automatizado en Fargate (solo Amazon ECS)	138
Agente automatizado en el recurso de Amazon EKS	174
Administración manual del agente para el clúster de Amazon EKS	213
Configurar los parámetros del complemento de EKS	222
Validar la configuración del punto de conexión de VPC	225
Problemas de la cobertura en tiempo de ejecución y resolución de problemas	227
Cobertura y resolución de problemas para los recursos de Amazon EC2	228
Cobertura y solución de problemas para clústeres de Amazon ECS	245

Cobertura y resolución de problemas para los clústeres de Amazon EKS	263
Configuración de la supervisión de la CPU y la memoria	279
Uso de VPC compartida	280
Funcionamiento	281
Requisitos previos	283
Utilizar laC con agentes automatizados	284
Información general sobre el gráfico de dependencia de recursos de laC	284
Problema común: eliminar recursos en laC	285
Tipos de eventos de tiempo de ejecución recopilados	286
Eventos de procesos	287
Eventos de contenedores	289
Eventos de tareas de AWS Fargate (solo en Amazon ECS)	289
Eventos de pod de Kubernetes	290
Eventos del sistema de nombres de dominio (DNS)	291
Eventos abiertos	292
Evento de carga de módulo	292
Eventos de Mprotect	292
Eventos de montaje	293
Eventos de enlace	293
Eventos de enlace simbólico	294
Eventos duplicados	294
Evento de mapa de memoria	295
Eventos de socket	295
Eventos de conexión	296
Eventos de Readv de VM de proceso	297
Eventos de Writev de VM de proceso	297
Eventos de rastreo de procesos (Ptrace)	298
Enviar de vinculación	298
Eventos de escucha	299
Eventos de cambio de nombre	300
Eventos de establecimiento de ID de usuario (UID)	300
Eventos chmod	301
Repositorio de Amazon ECR que aloja el agente de GuardDuty	301
Agentes de seguridad en el mismo host	313
Descripción general	313
Impact	313

Cómo GuardDuty gestiona a varios agentes	314
Supervisión en tiempo de ejecución de EKS	315
Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas (API)	315
Configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente (API)	358
Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución	366
Versiones del agente de seguridad de GuardDuty	370
Recursos adicionales: próximos pasos	401
Desactivar, desinstalar y limpiar recursos	401
Desinstalar manualmente el agente de seguridad para los recursos de Amazon EC2	403
Limpiar los recursos de los agentes de seguridad	405
Protección contra malware para EC2	407
Comparación del análisis de malware iniciado por GuardDuty y el análisis de malware bajo demanda	408
Cómo GuardDuty analiza los volúmenes de EBS para detectar malware	411
Volúmenes de EBS compatibles	412
Modificar el ID de clave de KMS predeterminada	413
Configure la retención de instantáneas y la cobertura de análisis de EC2	414
Retención de instantáneas	415
Opciones de análisis con etiquetas definidas por el usuario	416
Etiqueta GuardDutyExcluded global	420
Análisis de malware iniciado por GuardDuty	421
Prueba gratuita de 30 días	422
Habilitar el análisis de malware iniciado por GuardDuty en entornos de varias cuentas	423
Habilitar el análisis de malware iniciado por GuardDuty para una cuenta independiente	435
Resultados que invocan un análisis de malware iniciado por GuardDuty	436
Análisis de malware bajo demanda	438
Funcionamiento del análisis de malware bajo demanda	439
Inicio de un análisis de malware bajo demanda	440
Volver a analizar una instancia de Amazon EC2 previamente analizada	443
Supervisión de los estados y resultados de los análisis de malware	443
Cuentas de servicio de GuardDuty	445
Cuotas en la protección contra malware de EC2	449
Protección contra malware para S3	454

Precios y costo de uso	456
Revisar el costo de uso	457
Funcionamiento	457
Descripción general	457
Permisos de roles de IAM	457
Etiquetado opcional de objetos en función del resultado del análisis	458
Proceso posterior a la habilitación de la protección contra malware para S3 para un bucket	459
Capacidades de la protección contra malware para S3	461
(Opcional) Comience a utilizar la protección contra malware para S3 únicamente (consola)	462
Configurar la protección contra malware para S3 para el bucket	463
Habilitar la protección contra malware para la detección de amenazas de S3 para el bucket	464
Permisos de roles de IAM	471
Solución de problemas de errores de permisos de roles de IAM	476
Pasos a seguir tras habilitar la protección contra malware para S3	477
Utilizar el control de acceso basado en etiquetas (TBAC)	478
Agregar TBAC en el recurso del bucket de S3	479
Ver y entender el estado del bucket protegido	481
Solución de problemas sobre el estado del plan de protección contra malware	483
La notificación de EventBridge está desactivada para este bucket de S3	483
Falta la regla administrada por EventBridge para recibir eventos de buckets de S3	484
El bucket de S3 ya no existe	485
No se pudo colocar el objeto de prueba	485
Supervisión de los análisis de objetos de S3	487
Estado potencial de análisis de objeto de S3 y estado del producto	487
Uso de Amazon EventBridge	489
Utilizar etiquetas de objetos de S3	499
Usar alarmas y métricas de CloudWatch	500
Editar el plan de protección contra malware para un bucket protegido	503
Desactivar la protección contra malware para S3 para un bucket protegido	505
Compatibilidad con las características de Amazon S3	507
Protección contra malware para las cuotas de S3	515
Protección de RDS	519
Bases de datos compatibles	520
Actividad de inicio de sesión de RDS	521

Habilitar RDS Protection en entornos de varias cuentas	522
Habilitar RDS Protection para una cuenta independiente	529
Solución de problemas de monitoreo de protección de RDS	530
Almacenamiento de RDS completo	530
Versiones no compatibles en la base de datos principal de RDS para PostgreSQL	531
Consideraciones adicionales de seguridad	531
Protección de Lambda	533
Supervisión de la actividad de red de Lambda	534
Habilitar la protección de Lambda en entornos de varias cuentas	534
Habilitar la protección de Lambda para una cuenta independiente	542
Proteger las cargas de trabajo de IA	543
Múltiples cuentas en GuardDuty	544
Relaciones entre la cuenta de administrador y la cuenta de miembro	545
Administración de cuentas con AWS Organizations	549
Recomendaciones y consideraciones	550
Permisos necesarios para designar una cuenta de administrador delegado de GuardDuty ..	552
Designar cuenta de administrador delegado de GuardDuty	554
Configuración de las preferencias de habilitación automática de la organización	556
Cómo agregar miembros a la organización	560
(Opcional) Habilitar planes de protección para cuentas de miembro existentes	563
Administración continua de las cuentas de miembro en GuardDuty	563
Suspender GuardDuty para la cuenta de miembro	564
Desasociar (eliminar) la cuenta de miembro de la cuenta de administrador	566
Eliminar cuentas de miembro de la organización de GuardDuty	568
Cambiar la cuenta de administrador delegado de GuardDuty	570
Administración de cuentas por invitación	572
Agregar cuentas por invitación	573
Consolidación de cuentas de administrador bajo una sola organización	578
Consideraciones sobre GuardDuty para la opción Exportar CSV en las cuentas	581
Tipos de resultados	582
Tipos de resultados de EC2	582
Backdoor:EC2/C&CAActivity.B	584
Backdoor:EC2/C&CAActivity.B!DNS	585
Backdoor:EC2/DenialOfService.Dns	586
Backdoor:EC2/DenialOfService.Tcp	587
Backdoor:EC2/DenialOfService.Udp	588

Backdoor:EC2/DenialOfService.UdpOnTcpPorts	588
Backdoor:EC2/DenialOfService.UnusualProtocol	589
Backdoor:EC2/Spambot	590
Behavior:EC2/NetworkPortUnusual	590
Behavior:EC2/TrafficVolumeUnusual	591
CryptoCurrency:EC2/BitcoinTool.B	591
CryptoCurrency:EC2/BitcoinTool.B!DNS	592
DefenseEvasion:EC2/UnusualDNSResolver	593
DefenseEvasion:EC2/UnusualDoHActivity	593
DefenseEvasion:EC2/UnusualDoTActivity	594
Impact:EC2/AbusedDomainRequest.Reputation	595
Impact:EC2/BitcoinDomainRequest.Reputation	595
Impact:EC2/MaliciousDomainRequest.Reputation	596
Impact:EC2/MaliciousDomainRequest.Custom	597
Impact:EC2/PortSweep	597
Impact:EC2/SuspiciousDomainRequest.Reputation	598
Impact:EC2/WinRMBruteForce	599
Recon:EC2/PortProbeEMRUnprotectedPort	599
Recon:EC2/PortProbeUnprotectedPort	600
Recon:EC2/Portscan	601
Trojan:EC2/BlackholeTraffic	602
Trojan:EC2/BlackholeTraffic!DNS	602
Trojan:EC2/DGADomainRequest.B	603
Trojan:EC2/DGADomainRequest.C!DNS	604
Trojan:EC2/DNSDataExfiltration	605
Trojan:EC2/DriveBySourceTraffic!DNS	605
Trojan:EC2/DropPoint	606
Trojan:EC2/DropPoint!DNS	606
Trojan:EC2/PhishingDomainRequest!DNS	607
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	607
UnauthorizedAccess:EC2/MetadataDNSRebind	608
UnauthorizedAccess:EC2/RDPBruteForce	609
UnauthorizedAccess:EC2/SSHBruteForce	610
UnauthorizedAccess:EC2/TorClient	611
UnauthorizedAccess:EC2/TorRelay	612
Tipos de resultados de IAM	612

CredentialAccess:IAMUser/AnomalousBehavior	614
DefenseEvasion:IAMUser/AnomalousBehavior	614
Discovery:IAMUser/AnomalousBehavior	615
Exfiltration:IAMUser/AnomalousBehavior	616
Impact:IAMUser/AnomalousBehavior	617
InitialAccess:IAMUser/AnomalousBehavior	617
PenTest:IAMUser/KaliLinux	618
PenTest:IAMUser/ParrotLinux	619
PenTest:IAMUser/PentooLinux	619
Persistence:IAMUser/AnomalousBehavior	620
Policy:IAMUser/RootCredentialUsage	620
Policy:IAMUser/ShortTermRootCredentialUsage	621
PrivilegeEscalation:IAMUser/AnomalousBehavior	622
Recon:IAMUser/MaliciousIPCaller	623
Recon:IAMUser/MaliciousIPCaller.Custom	623
Recon:IAMUser/TorIPCaller	624
Stealth:IAMUser/CloudTrailLoggingDisabled	624
Stealth:IAMUser/PasswordPolicyChange	625
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	625
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	626
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	628
UnauthorizedAccess:IAMUser/MaliciousIPCaller	630
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	630
UnauthorizedAccess:IAMUser/TorIPCaller	631
Tipos de resultados de secuencias de ataque	631
AttackSequence:EKS/CompromisedCluster	632
AttackSequence:IAM/CompromisedCredentials	633
AttackSequence:S3/CompromisedData	633
Tipos de resultados de la S3 Protection	634
Discovery:S3/AnomalousBehavior	636
Discovery:S3/MaliciousIPCaller	636
Discovery:S3/MaliciousIPCaller.Custom	637
Discovery:S3/TorIPCaller	637
Exfiltration:S3/AnomalousBehavior	638
Exfiltration:S3/MaliciousIPCaller	639
Impact:S3/AnomalousBehavior.Delete	639

Impact:S3/AnomalousBehavior.Permission	640
Impact:S3/AnomalousBehavior.Write	641
Impact:S3/MaliciousIPCaller	642
PenTest:S3/KaliLinux	642
PenTest:S3/ParrotLinux	643
PenTest:S3/Pentoolinux	643
Policy:S3/AccountBlockPublicAccessDisabled	644
Policy:S3/BucketAnonymousAccessGranted	645
Policy:S3/BucketBlockPublicAccessDisabled	646
Policy:S3/BucketPublicAccessGranted	646
Stealth:S3/ServerAccessLoggingDisabled	647
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	648
UnauthorizedAccess:S3/TorIPCaller	648
Tipos de resultados de la protección de EKS	649
CredentialAccess:Kubernetes/MaliciousIPCaller	651
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	651
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	652
CredentialAccess:Kubernetes/TorIPCaller	653
DefenseEvasion:Kubernetes/MaliciousIPCaller	654
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	654
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	655
DefenseEvasion:Kubernetes/TorIPCaller	656
Discovery:Kubernetes/MaliciousIPCaller	656
Discovery:Kubernetes/MaliciousIPCaller.Custom	657
Discovery:Kubernetes/SuccessfulAnonymousAccess	658
Discovery:Kubernetes/TorIPCaller	659
Execution:Kubernetes/ExecInKubeSystemPod	659
Impact:Kubernetes/MaliciousIPCaller	660
Impact:Kubernetes/MaliciousIPCaller.Custom	661
Impact:Kubernetes/SuccessfulAnonymousAccess	661
Impact:Kubernetes/TorIPCaller	662
Persistence:Kubernetes/ContainerWithSensitiveMount	663
Persistence:Kubernetes/MaliciousIPCaller	664
Persistence:Kubernetes/MaliciousIPCaller.Custom	664
Persistence:Kubernetes/SuccessfulAnonymousAccess	665
Persistence:Kubernetes/TorIPCaller	666

Policy:Kubernetes/AdminAccessToDefaultServiceAccount	666
Policy:Kubernetes/AnonymousAccessGranted	667
Policy:Kubernetes/ExposedDashboard	668
Policy:Kubernetes/KubeflowDashboardExposed	668
PrivilegeEscalation:Kubernetes/PrivilegedContainer	669
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	669
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	670
Execution:Kubernetes/AnomalousBehavior.ExecInPod	671
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed! PrivilegedContainer	672
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount	673
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	674
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	676
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	677
Tipos de resultados de la supervisión en tiempo de ejecución	678
CryptoCurrency:Runtime/BitcoinTool.B	680
Backdoor:Runtime/C&CActivity.B	681
UnauthorizedAccess:Runtime/TorRelay	682
UnauthorizedAccess:Runtime/TorClient	682
Trojan:Runtime/BlackholeTraffic	683
Trojan:Runtime/DropPoint	684
CryptoCurrency:Runtime/BitcoinTool.B!DNS	684
Backdoor:Runtime/C&CActivity.B!DNS	685
Trojan:Runtime/BlackholeTraffic!DNS	687
Trojan:Runtime/DropPoint!DNS	687
Trojan:Runtime/DGADomainRequest.C!DNS	688
Trojan:Runtime/DriveBySourceTraffic!DNS	689
Trojan:Runtime/PhishingDomainRequest!DNS	690
Impact:Runtime/AbusedDomainRequest.Reputation	690
Impact:Runtime/BitcoinDomainRequest.Reputation	691
Impact:Runtime/MaliciousDomainRequest.Reputation	692
Impact:Runtime/SuspiciousDomainRequest.Reputation	693
UnauthorizedAccess:Runtime/MetadataDNSRebind	694
Execution:Runtime/NewBinaryExecuted	695
PrivilegeEscalation:Runtime/DockerSocketAccessed	696

PrivilegeEscalation:Runtime/RuncContainerEscape	697
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	698
DefenseEvasion:Runtime/ProcessInjection.Proc	699
DefenseEvasion:Runtime/ProcessInjection.Ptrace	700
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	700
Execution:Runtime/ReverseShell	701
DefenseEvasion:Runtime/FilelessExecution	702
Impact:Runtime/CryptoMinerExecuted	702
Execution:Runtime/NewLibraryLoaded	703
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	704
PrivilegeEscalation:Runtime/UserfaultfdUsage	704
Execution:Runtime/SuspiciousTool	705
Execution:Runtime/SuspiciousCommand	706
DefenseEvasion:Runtime/SuspiciousCommand	707
DefenseEvasion:Runtime/PtraceAntiDebugging	708
Execution:Runtime/MaliciousFileExecuted	709
Execution:Runtime/SuspiciousShellCreated	709
PrivilegeEscalation:Runtime/ElevationToRoot	710
Discovery:Runtime/SuspiciousCommand	711
Persistence:Runtime/SuspiciousCommand	712
PrivilegeEscalation:Runtime/SuspiciousCommand	713
DefenseEvasion:Runtime/KernelModuleLoaded	713
Tipos de resultados de la protección contra malware para EC2	714
Execution:EC2/MaliciousFile	715
Execution:ECS/MaliciousFile	715
Execution:Kubernetes/MaliciousFile	716
Execution:Container/MaliciousFile	716
Execution:EC2/SuspiciousFile	717
Execution:ECS/SuspiciousFile	718
Execution:Kubernetes/SuspiciousFile	718
Execution:Container/SuspiciousFile	719
Tipo de resultado de la protección contra malware para S3	720
Object:S3/MaliciousFile	720
Tipos de resultados de la protección de RDS	721
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	721
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	723

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	724
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	725
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	725
Discovery:RDS/MaliciousIPCaller	726
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	727
CredentialAccess:RDS/TorIPCaller.FailedLogin	727
Discovery:RDS/TorIPCaller	728
Tipos de resultados de la protección de Lambda	729
Backdoor:Lambda/C&CActivity.B	729
CryptoCurrency:Lambda/BitcoinTool.B	730
Trojan:Lambda/BlackholeTraffic	731
Trojan:Lambda/DropPoint	731
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	732
UnauthorizedAccess:Lambda/TorClient	732
UnauthorizedAccess:Lambda/TorRelay	733
Tipos de resultados retirados	733
Exfiltration:S3/ObjectRead.Unusual	734
Impact:S3/PermissionsModification.Unusual	735
Impact:S3/ObjectDelete.Unusual	736
Discovery:S3/BucketEnumeration.Unusual	737
Persistence:IAMUser/NetworkPermissions	737
Persistence:IAMUser/ResourcePermissions	738
Persistence:IAMUser/UserPermissions	739
PrivilegeEscalation:IAMUser/AdministrativePermissions	740
Recon:IAMUser/NetworkPermissions	741
Recon:IAMUser/ResourcePermissions	741
Recon:IAMUser/UserPermissions	742
ResourceConsumption:IAMUser/ComputeResources	743
Stealth:IAMUser/LoggingConfigurationModified	744
UnauthorizedAccess:IAMUser/ConsoleLogin	745
UnauthorizedAccess:EC2/TorIPCaller	745
Backdoor:EC2/XORDDOS	746
Behavior:IAMUser/InstanceLaunchUnusual	746
CryptoCurrency:EC2/BitcoinTool.A	747
UnauthorizedAccess:IAMUser/UnusualASNCaller	747
Tipos de resultados de GuardDuty por recursos potencialmente impactados	748

Tipos de resultados activos de GuardDuty	748
Comprender y generar resultados	771
Formato de resultado de GuardDuty	772
Propósitos de amenaza	774
Motor de análisis de detección de malware de GuardDuty	777
Hallazgos de ejemplo	777
Generación de resultados de muestra a través de la consola o la API de GuardDuty	778
Pruebe los resultados de GuardDuty	779
Consideraciones	780
El script de la herramienta de pruebas de resultados de GuardDuty puede generar	781
Paso 1: Requisitos previos	783
Paso 2: Implementar los recursos de AWS	784
Paso 3: Ejecute los scripts de la herramienta de pruebas	786
Paso 4: Limpiar los recursos de pruebas de AWS	788
Solución de problemas comunes	789
Página de resultados en la consola de GuardDuty	790
Navegación en la página Resultados	792
Niveles de gravedad de los resultados	793
Gravedad crítica	794
Gravedad alta	794
Gravedad media	794
Gravedad baja	795
Detalles de los resultados	795
Información general de los resultados	796
Recurso	797
Detalles de los resultados de la secuencia de ataque	805
Detalles de usuario de la base de datos (DB) de RDS	812
Detalles del resultado de la supervisión en tiempo de ejecución	812
Detalles del análisis de volúmenes de EBS	815
Detalles de los resultados de Malware Protection for EC2	816
Detalles de los resultados de la protección contra malware para S3	817
Acción	818
Actor u objetivo	819
Detalles de geolocalización	820
Información adicional	821
Evidencia	821

Comportamiento anómalo	822
Agregación de resultados de GuardDuty	827
Administrar los resultados de GuardDuty	829
Panel de resumen de GuardDuty	830
Descripción general	831
Resultados	832
Tipos de resultados más comunes	833
Resultados por gravedad	834
Cuentas con la mayoría de los resultados	834
Recursos con resultados	834
Resultados menos frecuentes	835
Cobertura de los planes de protección	835
Filtrar los resultados de GuardDuty	836
Creación y guardado de conjunto de filtros en la consola de GuardDuty	837
Crear y guardar un conjunto de filtros mediante la API y la CLI de GuardDuty	839
Filtros de propiedades en GuardDuty	841
Reglas de supresión	848
.....	848
Uso de reglas de supresión con Detección Extendida de Amenazas	849
Casos de uso comunes para reglas de supresión y ejemplos	850
Crear reglas de supresión	853
Eliminación de reglas de supresión	856
.....	855
Listas de entidades y listas de direcciones IP	858
Comprender las listas de entidades y listas de direcciones IP	858
Consideraciones importantes sobre las listas de GuardDuty	859
Formatos de las listas	860
Explicación de los estados de las listas	866
Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP ..	867
Añadir y activar una lista de entidades o una lista de IP	869
Actualización de una lista de entidades o una lista de direcciones IP	875
Desactivar la lista de entidades o la lista de direcciones IP	881
Eliminar la lista de entidades o la lista de direcciones IP	883
Exportar los resultados generados a Amazon S3	886
Consideraciones	887
Paso 1: Permisos necesarios para la exportación de resultados	888

Paso 2: Asociar la política a la clave de KMS	888
Paso 3: Asociar la política al bucket de Amazon S3	891
Paso 4: Exportar resultados a un bucket de S3 (consola)	894
Paso 5: Frecuencia de exportación de los resultados	896
Procesamiento de resultados con EventBridge	896
Frecuencia de notificaciones de EventBridge en GuardDuty	897
Configuración de un punto de conexión y un tema de Amazon SNS	898
Uso de EventBridge con GuardDuty	900
Creación de una regla de EventBridge	901
Regla de EventBridge para entornos de varias cuentas	908
Descripción de Registros de CloudWatch y motivos por los que omitir recursos	909
Auditar los registros de CloudWatch en Malware Protection for EC2 de GuardDuty	910
Retención de registros de Malware Protection for EC2 de GuardDuty	912
Motivos para omitir un recurso	912
Reportar un falso positivo en el producto del análisis de malware de EC2	918
Reportar un producto de análisis de objetos de S3 como falso positivo	919
Corrección de resultados	921
Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida	921
Corregir un bucket de S3 potencialmente comprometido	923
Recomendaciones basadas en las necesidades específicas de acceso al bucket de S3	925
Corregir un objeto de S3 potencialmente malicioso	926
Corregir un clúster de ECS potencialmente comprometido	926
Corregir credenciales de AWS potencialmente comprometidas	927
Corregir un contenedor independiente potencialmente comprometido	929
Corregir los resultados de EKS Protection	930
Posibles problemas de configuración	931
Corregir usuarios de Kubernetes potencialmente comprometidos	931
Corregir pods de Kubernetes potencialmente comprometidos	934
Corregir imágenes de contenedores potencialmente comprometidas	936
Corregir nodos de Kubernetes potencialmente comprometidos	937
Corregir los resultados de la Supervisión en tiempo de ejecución	937
Corrección de imágenes de contenedor en peligro	939
Corregir una base de datos potencialmente comprometida	940
Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos	940

Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos	941
Corrección de credenciales potencialmente en peligro	943
Restricción del acceso a la red	943
Corregir una función de Lambda potencialmente comprometida	944
Estimar el costo de uso	945
Descripción de cómo calcula GuardDuty los costos de uso	946
Supervisión en tiempo de ejecución: cómo los registros de flujo de VPC de las instancias de EC2 afectan al costo de uso	947
Cómo estima GuardDuty el costo del uso de los eventos de CloudTrail	947
Revisar el costo de uso estimado	947
Nombres de características para planes de protección en la API	950
Cambio de orígenes de datos a características	950
Cambios en la API de GuardDuty	950
Características en comparación con los orígenes de datos	951
Comprender cómo funcionan las API con características	952
Incorporar cambios de características en las API	952
Característica de asignaciones de GuardDuty	953
Seguridad	956
Protección de los datos	957
Cifrado en reposo	958
Cifrado en tránsito	958
Optar por no utilizar sus datos para mejorar el servicio	958
Registro con CloudTrail	960
Información de GuardDuty en CloudTrail	960
Eventos del plano de control de GuardDuty en CloudTrail	961
Eventos de datos de GuardDuty en CloudTrail	962
Ejemplo: entradas de archivos de registro de GuardDuty	963
Identity and Access Management	965
Público	966
Autenticación con identidades	966
Administración de acceso mediante políticas	968
Cómo funciona Amazon GuardDuty con IAM	970
Ejemplos de políticas basadas en identidades	975
Cómo utilizar roles vinculados a servicios	985

Políticas gestionadas de AWS	996
Solución de problemas	1006
Validación de conformidad	1008
Resiliencia	1009
Seguridad de la infraestructura	1009
Puntos de conexión de VPC (AWS PrivateLink)	1010
Consideraciones sobre los puntos de conexión de VPC de GuardDuty	1010
Crear un punto de conexión de VPC de interfaz para GuardDuty	1010
Crear una política de punto de conexión de VPC para GuardDuty	1011
Subredes compartidas	1011
Integración con los servicios de seguridad de AWS	1013
Integración de GuardDuty con AWS Security Hub CSPM	1013
Integración de GuardDuty con Amazon Detective	1013
AWS Security Hub CSPM Integración de	1013
Cómo envía Amazon GuardDuty los resultados a AWS Security Hub CSPM	1014
Visualización de los resultados de GuardDuty en AWS Security Hub CSPM	1015
Habilitación y configuración de la integración	1034
Utilizar controles de GuardDuty en Security Hub	1035
Detención de la publicación de resultados en Security Hub	1035
Integración con Amazon Detective	1035
Habilitación de la integración	1036
Paso de un resultado de GuardDuty a Amazon Detective	1036
Uso de la integración con un entorno multicuenta de GuardDuty	1037
Suspensión o deshabilitación	1038
Anuncios para GuardDuty	1040
Formato de los mensajes de Amazon SNS	1046
Cuotas de GuardDuty	1052
Solución de problemas	1058
Exportar resultados a Amazon S3: error de acceso	1058
Problemas de la protección contra malware para EC2	1059
Falta el permiso de administración AWS Organizations necesario al habilitar el análisis de malware iniciado por GuardDuty	1059
Estoy iniciando un análisis de malware bajo demanda, pero se produce un error de falta de permisos necesarios.	1059
Recibo un error iam:GetRole al trabajar con la protección contra malware para EC2.	1059

Soy una cuenta de administrador de GuardDuty que necesita habilitar el análisis de malware iniciado por GuardDuty pero no utiliza la política administrada de AWS:	
AmazonGuardDutyFullAccess para administrar GuardDuty.	1060
Problemas de supervisión en tiempo de ejecución	1060
Problemas de cobertura en tiempo de ejecución	1060
Solución de problemas de memoria insuficiente	1060
Se producen errores inesperados en mi flujo de trabajo de AWS Step Functions	1061
Otras cuestiones de solución de problemas	1062
Regiones y puntos de conexión	1063
Disponibilidad de características específicas por región	1063
Acciones y parámetros heredados	1065
Historial de revisión	1067
Actualizaciones anteriores	1170

¿Qué es Amazon GuardDuty?

Amazon GuardDuty es un servicio de detección de amenazas que supervisa, analiza y procesa continuamente los orígenes de datos de AWS y los registros del entorno de AWS. GuardDuty utiliza fuentes de inteligencia de amenazas, como listas de direcciones IP y dominios maliciosos, hashes de archivos y modelos de machine learning (ML) para identificar actividades sospechosas y potencialmente maliciosas en el entorno de AWS. En la siguiente lista se proporciona información general sobre los posibles escenarios de amenazas que GuardDuty puede ayudar a detectar:

- Credenciales de AWS comprometidas y filtradas.
- Filtración y destrucción de datos que puede conducir a un evento de ransomware. Patrones inusuales de eventos de inicio de sesión en versiones de motor compatibles de bases de datos de Amazon Aurora y Amazon RDS, que indican un comportamiento anómalo.
- Actividad de minería de criptomonedas no autorizada en las instancias y cargas de trabajo de contenedores de Amazon Elastic Compute Cloud (Amazon EC2).
- Presencia de malware en las instancias de Amazon EC2 y en las cargas de trabajo de contenedores, así como en los archivos recién cargados en los buckets de Amazon Simple Storage Service (Amazon S3).
- Eventos a nivel de sistema operativo, redes y archivos que indiquen un comportamiento no autorizado en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS), tareas de AWS Fargate Amazon Elastic Container Service (Amazon ECS) e instancias y cargas de trabajo de contenedores de Amazon EC2 .

En el siguiente video se ofrece información general sobre cómo GuardDuty ayuda a detectar amenazas en el entorno de AWS.

[¿Qué es Amazon GuardDuty?](#)

Contenido

- [Características de GuardDuty](#)
- [Conformidad con DSS de PCI](#)
- [Precios en GuardDuty](#)
- [Acceso a GuardDuty](#)

Características de GuardDuty

Estas son algunas de las formas clave en las que Amazon GuardDuty ayuda a supervisar, detectar y administrar posibles amenazas en el entorno de AWS.

Supervisa continuamente orígenes de datos y registros de eventos específicos

- **Detección de amenazas fundamentales:** al habilitar GuardDuty en una Cuenta de AWS, este comienza automáticamente a ingerir los orígenes de datos fundamentales asociados con dicha cuenta. Estos orígenes de datos incluyen eventos de administración de AWS CloudTrail, registros de flujo de VPC (de instancias de Amazon EC2) y registros de DNS. No necesita habilitar nada más para que GuardDuty comience a analizar y procesar estos orígenes de datos para generar resultados de seguridad asociados. Para obtener más información, consulte [Orígenes de datos fundamentales de GuardDuty](#).
- **Detección Extendida de Amenazas:** esta capacidad detecta ataques en varias etapas que abarcan orígenes de datos fundamentales, varios tipos de recursos de AWS y tiempo, dentro de una Cuenta de AWS. Es posible que haya varios eventos en su cuenta que, por separado, no se presenten como una amenaza clara. Sin embargo, cuando estos eventos se observan en una secuencia que indica una actividad sospechosa, GuardDuty la identifica como una secuencia de ataque. GuardDuty lo notifica mediante la generación del tipo de resultado de secuencia de ataque asociado para proporcionar detalles sobre la secuencia de ataque observada.

Sin costo adicional, la Detección Extendida de Amenazas se activa automáticamente para cada Cuenta de AWS cuando activan GuardDuty. Esta capacidad no requiere que habilite ningún plan de protección centrado en los casos de uso. Sin embargo, para aumentar el alcance de la seguridad de sus recursos de Amazon S3, GuardDuty recomienda habilitar la S3 Protection en su cuenta. Esto ayudará a que la Detección Extendida de Amenazas identifique los ataques en varias etapas que podrían afectar a sus recursos de Amazon S3.

Para obtener más información acerca de cómo funciona esta característica y qué escenarios de amenaza cubre, consulte [Detección Extendida de Amenazas de GuardDuty](#).

- **Planes de protección GuardDuty centrados en casos de uso:** para mejorar la visibilidad de detección de amenazas en la seguridad del entorno de AWS, GuardDuty ofrece planes de protección dedicados que puede optar por habilitar. Los planes de protección ayudan a supervisar los registros y eventos de otros servicios de AWS. Estos orígenes incluyen registros de auditoría de EKS, actividad de inicio de sesión en RDS, eventos de datos de Amazon S3 en CloudTrail, volúmenes de EBS, Supervisión en tiempo de ejecución en Amazon EKS, Amazon

EC2 y Amazon ECS-Fargate, así como registros de actividad de red de Lambda. GuardDuty consolida estos registros y orígenes de eventos bajo el término: [características](#). Puede habilitar uno o más planes de protección dedicados en una Región de AWS compatible en cualquier momento. GuardDuty comenzará a supervisar, procesar y analizar las actividades en función del plan de protección que habilite. Para obtener más información sobre cada plan de protección y su funcionamiento, consulte el documento del plan de protección correspondiente.

Plan de protección	Descripción
Protección de S3	Identifica posibles riesgos de seguridad, como intentos de filtración y destrucción de datos en los buckets de Amazon S3.
EKS Protection	La supervisión de registros de auditoría de EKS analiza los registros de auditoría de Kubernetes de los clústeres de Amazon EKS en busca de actividades potencialmente sospechosas y maliciosas.
Supervisión en tiempo de ejecución	Supervisa y analiza eventos a nivel de sistema operativo en Amazon EKS, Amazon EC2 y Amazon ECS (incluido AWS Fargate) para detectar posibles amenazas en tiempo de ejecución.
Protección contra malware para EC2	Detecta la posible presencia de malware mediante el análisis de los volúmenes de Amazon EBS asociados a las instancias de Amazon EC2. Existe la opción de utilizar esta característica bajo demanda.
Protección contra malware para S3	Detecta la posible presencia de malware en los objetos recién cargados en los buckets de Amazon S3.
Protección de RDS	Analiza la actividad de inicio de sesión en RDS y elabora perfiles para detectar posibles amenazas de acceso a las bases de datos compatibles de Amazon Aurora y Amazon RDS.

Plan de protección	Descripción
Protección de Lambda	Supervisa los registros de actividad de red de Lambda, a partir de los registros de flujo de VPC, con el fin de detectar amenazas a las funciones de AWS Lambda. Entre las amenazas potenciales figuran la minería de criptomonedas y la comunicación con servidores maliciosos.

 Habilitar la protección contra malware para S3 de forma independiente

GuardDuty brinda flexibilidad para utilizar la protección contra malware para S3 de forma independiente, sin habilitar el servicio de Amazon GuardDuty. Para obtener más información sobre cómo comenzar a utilizar únicamente la protección contra malware para S3, consulte [Protección contra malware para S3 de GuardDuty](#). Para utilizar todos los demás planes de protección, debe habilitar el servicio de GuardDuty.

Administre un entorno de varias cuentas

Puede administrar un entorno de AWS de varias cuentas ya sea mediante AWS Organizations (opción recomendada) o a través del tradicional método por invitación. Para obtener más información, consulte [Múltiples cuentas en GuardDuty](#).

Genera resultados de seguridad para las amenazas detectadas

Cuando GuardDuty detecta amenazas potenciales a la seguridad asociadas a los recursos de AWS, comienza a generar resultados de seguridad que brindan información sobre el recurso potencialmente comprometido. Después de habilitar GuardDuty en la cuenta, genere [Hallazgos de ejemplo](#) para ver el [Detalles de los resultados](#) asociado. Para obtener una lista completa de los resultados de seguridad, consulte [Tipos de resultados de GuardDuty](#).

Con GuardDuty, también puede usar un script de herramienta de pruebas que genere resultados de seguridad específicos de GuardDuty para comprender cómo revisar los resultados de GuardDuty y responder ante estos. Para obtener más información, consulte [Pruebe los resultados de GuardDuty en cuentas dedicadas](#).

Evaluar y administrar los resultados de seguridad

GuardDuty consolida los resultados de seguridad de las cuentas y muestra el producto en el panel de resumen de la Consola de GuardDuty. También puede recuperar los resultados a través

de la API AWS Security Hub CSPM, AWS Command Line Interface o el SDK de AWS. Gracias a una perspectiva integral del estado actual de la seguridad, podrá identificar tendencias y posibles problemas, además de implementar las medidas correctivas necesarias. Para obtener más información, consulte [Administrar los resultados de GuardDuty](#).

Integración con los servicios de seguridad de AWS relacionados

Para facilitar aún más el análisis y la investigación de las tendencias de seguridad en el entorno de AWS, considere la posibilidad de utilizar los siguientes servicios de AWS relacionados con la seguridad en combinación con GuardDuty.

- **AWS Security Hub CSPM:** este servicio ofrece una visión completa del estado de seguridad de los recursos de AWS, a la vez que ayuda a comprobar el entorno de AWS respecto a las prácticas recomendadas y los estándares del sector de seguridad. Para ello, entre otras cosas, consume, agrega, organiza y prioriza los resultados de seguridad de múltiples servicios de AWS (incluido Amazon Macie) y productos compatibles de la red de socios de AWS (APN). Security Hub lo ayuda a analizar sus tendencias de seguridad para identificar y dar prioridad a los problemas de seguridad en su entorno de AWS.

Para obtener información sobre el uso conjunto de GuardDuty y Security Hub, consulte [Integración de GuardDuty con AWS Security Hub CSPM](#). Para obtener más información sobre Security Hub, consulte la [Guía del usuario de AWS Security Hub CSPM](#).

- **Amazon Detective:** este servicio ayuda a analizar, investigar e identificar rápidamente la causa raíz de los resultados de seguridad o las actividades sospechosas. Detective recopila automáticamente los datos de registro de sus recursos de AWS. A continuación, utiliza el machine learning, el análisis estadístico y la teoría de grafos para generar visualizaciones que lo ayuden a realizar investigaciones sobre la seguridad con mayor rapidez y de forma más eficaz. Las agregaciones de datos, resúmenes y contexto predefinidos de Detective ayudan a analizar los posibles problemas de seguridad, así como a determinar su naturaleza y alcance.

Para obtener información sobre cómo utilizar GuardDuty y Detective conjuntamente, consulte [Integración de GuardDuty con Amazon Detective](#). Para obtener más información sobre Detective, consulte la [Guía del usuario de Amazon Detective](#).

- **Amazon EventBridge:** este servicio facilita la recepción de notificaciones y la respuesta a los resultados de seguridad de GuardDuty casi en tiempo real. GuardDuty crea un evento cuando se produce un cambio en los resultados. Puede seleccionar la frecuencia con la que desea recibir las notificaciones de EventBridge. Para obtener más información, consulte [¿Qué es Amazon EventBridge?](#) en la Guía del usuario de Amazon EventBridge.

Conformidad con DSS de PCI

GuardDuty admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios. Además, se ha validado como conforme al estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI). Para obtener más información acerca de PCI DSS, incluido cómo solicitar una copia del Paquete de conformidad con PCI de AWS, consulte [PCI DSS Nivel 1](#).

Para obtener más información, consulte [Nueva prueba realizada por un tercero compara Amazon GuardDuty con los sistemas de detección de intrusiones en la red](#) en el Blog de seguridad de AWS.

Precios en GuardDuty

Esta sección se centra en el modelo capa gratuita de AWS que utiliza GuardDuty para los distintos planes de protección y en cómo puede ver los costos de uso estimados y reales. Si busca información sobre los precios asociados a todos los planes de protección de las regiones compatibles, consulte los [precios de GuardDuty](#).

capa gratuita de AWS

capa gratuita de AWS ayuda a explorar y probar Servicios de AWS de forma gratuita hasta los límites especificados para cada servicio. Existen tres categorías: 12 meses gratis, siempre gratis y pruebas gratuitas de corta duración. Amazon GuardDuty forma parte de la categoría de pruebas gratuitas a corto plazo y ofrece un periodo de prueba gratuita de 30 días. Si continúa con el uso de GuardDuty una vez finalizada la prueba gratuita, comenzará a incurrir en cargos en función del uso que haga de este servicio.

¹ Excepción a la prueba gratuita de 30 días de GuardDuty

El análisis de malware bajo demanda (bajo Malware Protection for EC2) y la protección contra malware para S3 no forman parte de la categoría de prueba gratuita de 30 días de GuardDuty. La protección contra malware para S3 forma parte de la categoría de gratuidad de 12 meses del capa gratuita de AWS, mientras que el análisis de malware bajo demanda se basa en un modelo de pago por uso. No se ofrece una prueba gratuita de 30 días ni un modelo de costo de nivel gratuito de 12 meses para el análisis de malware bajo demanda.

Utilizar la prueba gratuita de 30 días de GuardDuty

Al usar GuardDuty por primera vez en una Región de AWS, la Cuenta de AWS se inscribe automáticamente en una prueba gratuita de 30 días en esa región. Algunos de los planes de protección también se habilitarán automáticamente y están incluidos en la prueba gratuita de 30 días. Debido a que GuardDuty es un servicio regional, cuando se habilita por primera vez en una región diferente, la cuenta obtendrá una prueba gratuita de 30 días de GuardDuty en esa región. Cuando se trabaja con varias cuentas en una organización de GuardDuty, cada una recibe su propia prueba gratuita de 30 días.

Utilice la siguiente tabla para revisar qué planes de protección están habilitados de forma predeterminada con GuardDuty y su disponibilidad de prueba gratuita.

Plan de protección	Habilitado de forma predeterminada con GuardDuty	Disponibilidad de prueba gratuita independiente ²	
EKS Protection	Sí	Sí	
Protección de S3	Sí	Sí	
Supervisión en tiempo de ejecución	No	Sí	
Protección contra malware para EC2 – Análisis de malware iniciado por GuardDuty	Sí	Sí	
Protección contra malware para EC2 – Análisis de malware bajo demanda en GuardDuty	No	No ¹	

Plan de protección	Habilitado de forma predeterminada con GuardDuty	Disponibilidad de prueba gratuita independiente ²	
Protección contra malware para S3 de GuardDuty	No	No ¹	
Protección de RDS	Sí	Sí	
Protección de Lambda	Sí	Sí	

²Al habilitar GuardDuty por primera vez, los planes de protección (excepto Runtime Monitoring) se habilitan automáticamente y se incluyen en la prueba gratuita inicial de 30 días. Cuando una cuenta de GuardDuty existente habilita un nuevo plan de protección después de que haya expirado la prueba gratuita inicial de GuardDuty, ese plan de protección incluye su propia prueba gratuita de 30 días. Para obtener más información sobre las pruebas gratuitas de los planes de protección, consulte el documento relacionado con cada plan de protección.

Vea el costo de uso estimado durante la prueba gratuita: durante los 30 días de prueba gratuita de GuardDuty, y en caso de habilitar un plan de protección, GuardDuty proporciona una estimación del costo de uso asociado a la cuenta. Si es una cuenta de administrador delegado de GuardDuty, puede ver el costo total estimado de uso y el desglose a nivel de cuenta para todas las cuentas de miembro que han habilitado GuardDuty. Para obtener más información, consulte [Estimar el costo de uso de GuardDuty](#).

Costo de uso una vez finalizada la prueba gratuita: si continúa con el uso de GuardDuty o de cualquiera de sus planes de protección una vez finalizada la prueba gratuita, empezará a incurrir en cargos por uso asociados. Para consultar la factura, vaya al Explorador de costos en la Consola <https://console.aws.amazon.com/costmanagement/>. Para obtener más información sobre la facturación de la cuenta de AWS, consulte la [Guía del usuario de AWS Billing](#).

Utilizar la protección contra malware para S3 con el nivel gratuito de 12 meses

La protección contra malware para S3 utiliza un plan de nivel gratuito asociado a las Cuentas de AWS que sean nuevas, tengan un nivel gratuito activo o cuyo nivel gratuito de 12 meses haya expirado. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).

Acceso a GuardDuty

Amazon GuardDuty está disponible en la mayoría de Regiones de AWS. Para obtener una lista de las regiones en las que GuardDuty está disponible, consulte [Regiones y puntos de conexión](#).

Puede utilizar GuardDuty de cualquiera de las siguientes formas:

Consola de GuardDuty

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

La consola es una interfaz basada en navegador para acceder a GuardDuty y utilizar dicho servicio. La consola de GuardDuty proporciona acceso a la cuenta, los datos y los recursos de GuardDuty.

AWS Command Line Interface

Con AWS Command Line Interface (AWS CLI), puede emitir comandos en la línea de comandos del sistema para llevar a cabo tareas de GuardDuty y tareas de AWS. Los comandos de la AWS CLI son útiles si desea crear scripts que lleven a cabo tareas.

Para obtener información sobre la instalación y el uso de la AWS CLI, consulte la [Guía del usuario de la AWS Command Line Interface](#). Para consultar los comandos de la AWS CLI disponibles para GuardDuty, consulte la [Referencia de comandos de la AWS CLI](#).

API HTTPS de GuardDuty

Puede acceder a GuardDuty y AWS mediante programación con la API HTTPS de GuardDuty, que le permite emitir solicitudes HTTPS directamente al servicio. Para obtener más información, consulte la [Referencia de la API de Amazon GuardDuty](#).

AWS SDK

AWS ofrece kits de desarrollo de software (SDK) que se componen de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas (Java, Python, Ruby, .NET, iOS, Android, etc.). Los SDK permiten crear cómodamente acceso mediante programación a GuardDuty. Para obtener información sobre los SDK de AWS (por ejemplo, cómo descargarlos e instalarlos), consulte [Herramientas para Amazon Web Services](#).

Conceptos y términos clave de Amazon GuardDuty

Conforme comienza a utilizar Amazon GuardDuty, puede beneficiarse de conocer sus conceptos y términos clave asociados.

Cuenta de

Cuenta estándar de Amazon Web Services (AWS) que contiene los recursos de AWS. Puede iniciar sesión en AWS con su cuenta y habilitar GuardDuty.

También puede invitar a otras cuentas a habilitar GuardDuty y asociarse con su cuenta de AWS en GuardDuty. Si se aceptan las invitaciones, la cuenta se designa como cuenta de administrador de GuardDuty, y las cuentas agregadas se convierten en las cuentas de miembro. A continuación, podrá ver y administrar los resultados de GuardDuty de estas cuentas en su nombre.

Los usuarios de la cuenta de administrador pueden configurar GuardDuty, así como ver y administrar los resultados de este servicio en sus propias cuentas y todas las cuentas de sus miembros. Para obtener información sobre la cantidad de cuentas de miembro que puede administrar la cuenta de administrador, consulte [Cuotas de GuardDuty](#).

Los usuarios de las cuentas de miembro pueden configurar GuardDuty y pueden ver y administrar los resultados de este servicio en su cuenta (ya sea a través de la consola de administración o la API de GuardDuty). Los usuarios de cuentas de miembros no pueden ver ni administrar los resultados de las cuentas de otros miembros.

Una Cuenta de AWS no puede ser cuenta de administrador y cuenta de miembro de GuardDuty al mismo tiempo. Una Cuenta de AWS solo puede aceptar una invitación de membresía. La aceptación de una invitación de suscripción es opcional.

Para obtener más información, consulte [Múltiples cuentas en Amazon GuardDuty](#).

Secuencia de ataque

Una secuencia de ataque es una correlación de varios eventos que, como observó GuardDuty, ocurrieron en una secuencia específica que coincide con el patrón de una actividad sospechosa. GuardDuty utiliza su capacidad [Detección Extendida de Amenazas](#) para detectar estos ataques en varias etapas que abarcan los orígenes de datos, los recursos de AWS y el cronograma fundamentales de su cuenta.

La siguiente lista explica brevemente los términos clave asociados a las secuencias de ataque:

- **Indicadores:** proporcionan información sobre por qué una secuencia de eventos se alinea con una posible actividad sospechosa.
- **Señales:** una señal es una actividad de la API que GuardDuty ha observado o un resultado de GuardDuty ya detectado en su cuenta. Al correlacionar los eventos observados en una secuencia específica en la cuenta, GuardDuty identifica una secuencia de ataque.

Hay eventos en su cuenta que no son indicativos de una amenaza potencial. GuardDuty las considera señales débiles. Sin embargo, cuando se observan señales débiles y resultados de GuardDuty en una secuencia específica que, cuando se correlacionan, se alinean con una actividad potencialmente sospechosa, GuardDuty genera un resultado de secuencia de ataque.

- **Puntos de conexión:** información sobre los puntos de conexión de la red que un actor de amenazas podría utilizar en una secuencia de ataque.

Detector

Amazon GuardDuty es un servicio regional. Al habilitar GuardDuty en una determinada Región de AWS, un ID de detector se asocia a la Cuenta de AWS. Este identificador alfanumérico de 32 caracteres es único para la cuenta en esa región. Por ejemplo, al habilitar GuardDuty para la misma cuenta en una región diferente, un ID de detector diferente se asociará a la cuenta. El formato de un `detectorId` es `12abc34d567e8fa901bc2d34e56789f0`.

Todos los resultados, cuentas y acciones de GuardDuty relacionadas con la administración de resultados y el servicio de GuardDuty utilizan el ID del detector para ejecutar una operación de la API.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Note

En entornos multicuenta, todos los resultados para las cuentas de miembro se agregan al detector de la cuenta de administrador.

Algunas funcionalidades de GuardDuty se configuran a través del detector, como la configuración de la frecuencia de las notificaciones de Eventos de CloudWatch, y la habilitación o desactivación de planes de protección opcionales para que GuardDuty los procese.

Usar la protección contra malware para S3 en GuardDuty

Al habilitar la protección contra malware para S3 en una cuenta en la que GuardDuty está habilitado, las acciones de protección contra malware para S3, como habilitar, editar y desactivar un recurso protegido, no se asocian con el ID del detector.

Cuando no habilita GuardDuty y elige la opción de detección de amenazas de la protección contra malware para S3, no se crea ningún ID de detector para la cuenta.

Orígenes de datos fundamentales

El origen o la ubicación de un conjunto de datos. Para detectar una actividad no autorizada o inesperada en su entorno de AWS. GuardDuty analiza y procesa datos de registros de eventos de AWS CloudTrail, eventos de administración de AWS CloudTrail, eventos de datos de AWS CloudTrail para S3, registros de flujo de VPC, registros de DNS. Consulte [Orígenes de datos fundamentales de GuardDuty](#).

Característica

Un objeto de característica configurado para su plan de protección de GuardDuty ayuda a detectar una actividad no autorizada o inesperada en su entorno de AWS. Cada plan de protección de GuardDuty configura el objeto de característica correspondiente para analizar y procesar datos. Algunos de los objetos de características son los registros de auditoría de EKS, la supervisión de la actividad de inicio de sesión en RDS, los registros de actividad de red de Lambda y los volúmenes de EBS. Para obtener más información, consulte [Nombres de características para planes de protección en la API de GuardDuty](#).

Resultado

Un problema de seguridad potencial detectado por GuardDuty. Para obtener más información, consulte [Comprender y generar resultados de Amazon GuardDuty](#).

Los resultados se muestran en la consola de GuardDuty y contienen una descripción detallada del problema de seguridad. También puede recuperar los resultados generados al llamar a las operaciones de la API [GetFindings](#) y [ListFindings](#).

También puede ver los resultados de GuardDuty en los eventos de Amazon CloudWatch. GuardDuty envía los resultados a Amazon CloudWatch mediante el protocolo HTTPS. Para obtener más información, consulte [Procesamiento de resultados de GuardDuty con Amazon EventBridge](#).

rol de IAM

Este es el rol de IAM con los permisos requeridos para analizar el objeto de S3. Cuando el etiquetado de objetos analizados está habilitado, los permisos de IAM PassRole ayudan a GuardDuty a agregar etiquetas al objeto analizado.

Recurso del plan de protección contra malware

Después de habilitar la protección contra malware para S3 para un bucket, GuardDuty crea un recurso del plan de protección contra malware. Este recurso está asociado al ID del plan de protección contra malware, que es un identificador único del bucket protegido. Utilice el recurso del plan de protección contra malware para realizar operaciones de la API en un recurso protegido.

Bucket protegido (recurso protegido)

Se considera que un bucket de Amazon S3 está protegido cuando habilita la protección contra malware para S3 para este bucket y su estado de protección cambia a Activo.

GuardDuty admite únicamente un bucket de S3 como recurso protegido.

Estado de protección

El estado asociado al recurso del plan de protección contra malware. Después de habilitar la protección contra malware para S3 para el bucket, este estado representa si el bucket está configurado correctamente o no.

Prefijo del objeto de S

En un bucket de Amazon Simple Storage Service (Amazon S3), puede utilizar prefijos para organizar el almacenamiento. Un prefijo es una agrupación lógica de los objetos de un bucket de S3. Para obtener más información, consulte [Organización y enumeración de objetos](#) en la Guía del usuario de Amazon S3.

Opciones de análisis

Cuando Malware Protection for EC2 de GuardDuty está habilitada, permite especificar qué instancias de Amazon EC2 y volúmenes de Amazon Elastic Block Store (EBS) debe analizar u omitir. Esta característica le permite agregar las etiquetas existentes que están asociadas a las instancias de EC2 y al volumen de EBS a una lista de etiquetas de inclusión o a una lista de etiquetas de exclusión. Los recursos asociados a las etiquetas que agregue a una lista de etiquetas de inclusión se analizan en busca de malware y los que se agregan a una lista de etiquetas de exclusión no se analizan. Para obtener más información, consulte [Opciones de análisis con etiquetas definidas por el usuario](#).

Retención de instantáneas

Cuando Malware Protection for EC2 de GuardDuty está habilitada, brinda la opción de retener las instantáneas de los volúmenes de EBS en la cuenta de AWS. GuardDuty genera las réplicas de los volúmenes de EBS en función de las instantáneas de dichos volúmenes. Puede retener las instantáneas de los volúmenes de EBS solo si el análisis de Malware Protection for EC2 detecta malware en las réplicas de los volúmenes de EBS. Si no se detecta ningún malware en las réplicas de los volúmenes de EBS, GuardDuty elimina automáticamente las instantáneas de dichos volúmenes, independientemente de la configuración de retención de instantáneas. Para obtener más información, consulte [Retención de instantáneas](#).

Regla de supresión de

Las reglas de supresión permiten crear combinaciones de atributos muy específicas para suprimir los resultados. Por ejemplo, puede definir una regla a través del filtro de GuardDuty para archivar automáticamente Recon:EC2/Portscan solo de aquellas instancias que estén en una VPC determinada, que ejecuten una AMI específica o con una etiqueta de EC2 específica. Esta regla daría lugar a que los resultados del escaneo de puertos se archivaran automáticamente desde las instancias que cumplan los criterios. Sin embargo, sigue permitiendo la generación de alertas si GuardDuty detecta que esas instancias están llevando a cabo otras actividades maliciosas; por ejemplo, la extracción de criptomonedas.

Las reglas de supresión definidas en la cuenta de administrador de GuardDuty se aplican a las cuentas de miembro de este servicio. Las cuentas de miembro de GuardDuty no pueden modificar las reglas de supresión.

Con las reglas de supresión, GuardDuty sigue generando todos los resultados. Las reglas de supresión facilitan la eliminación de resultados, mientras mantienen un historial completo e inmutable de todas las actividades.

Normalmente, las reglas de supresión se utilizan para ocultar los hallazgos del entorno que se consideran falsos positivos y reducir así el ruido de los resultados con poco valor para que pueda centrarse en amenazas más importantes. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Lista de IP de confianza

Una lista de direcciones IP de confianza para facilitar una comunicación de gran seguridad con el entorno de AWS. GuardDuty no genera resultados en función de las listas de IP de confianza. Para obtener más información, consulte [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#).

Lista de IP de amenazas

Una lista de direcciones IP maliciosas conocidas. Además de generar resultados debido a una actividad potencialmente sospechosa, GuardDuty también genera resultados en función de estas listas de amenazas. Para obtener más información, consulte [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#).

Introducción a GuardDuty

En este tutorial, encontrará una introducción práctica acerca de GuardDuty. Los requisitos mínimos para habilitar GuardDuty como una cuenta independiente o como administrador de GuardDuty con AWS Organizations se describen en el paso 1. Los pasos del 2 a 5 incluyen el uso de las características adicionales recomendadas por GuardDuty para aprovechar al máximo sus resultados.

Temas

- [Antes de empezar](#)
- [Paso 1: habilitación de Amazon GuardDuty](#)
- [Paso 2: generación de resultados de muestra y exploración de las operaciones básicas](#)
- [Paso 3: configuración de la exportación de los resultados de GuardDuty a un bucket de Amazon S3](#)
- [Paso 4: configuración de alertas de resultados de GuardDuty a través de SNS](#)
- [Pasos a seguir a continuación](#)

Antes de empezar

GuardDuty es un servicio de detección de amenazas que monitorea [Orígenes de datos fundamentales](#) como eventos de administración de AWS CloudTrail, registros de flujo de Amazon VPC y registros de consulta de DNS Amazon Route 53 Resolver. GuardDuty también analiza las características asociadas a sus tipos de protección solo si las habilita por separado. Las [características](#) incluyen los registros de auditoría de Kubernetes, la actividad de inicio de sesión de RDS, los eventos de datos de AWS CloudTrail de Amazon S3, los volúmenes de Amazon EBS, el monitoreo del tiempo de ejecución y los registros de actividad de la red de Lambda. Con estos orígenes de datos y características (si se han habilitado), GuardDuty genera resultados de seguridad para su cuenta.

Después de activar GuardDuty, comienza a monitorear su cuenta en busca de amenazas potenciales en función de las actividades en los orígenes de datos fundamentales. De forma predeterminada, [Detección Extendida de Amenazas](#) está habilitada para todas las Cuentas de AWS que tienen GuardDuty activado. Esta capacidad detecta secuencias de ataques en varias etapas que abarcan varios orígenes de datos fundamentales, recursos de AWS y el tiempo en su cuenta. Para detectar posibles amenazas a recursos de AWS específicos, puede optar por habilitar los planes de

protección centrados en casos de uso que ofrece GuardDuty. Para obtener más información, consulte [Características de GuardDuty](#).

No necesita habilitar ninguno de los orígenes de datos fundamentales de forma explícita. Al habilitar la S3 Protection, no es necesario habilitar explícitamente el registro de eventos de datos de Amazon S3. Del mismo modo, al habilitar EKS Protection, no es necesario habilitar explícitamente los registros de auditoría de Amazon EKS. Amazon GuardDuty extrae secuencias independientes de datos directamente de estos servicios.

En el caso de una cuenta nueva de GuardDuty, algunos de los tipos de protección disponibles que son admitidos en una Región de AWS están habilitados e incluidos de forma predeterminada en el periodo de prueba gratuito de 30 días. Puede excluirse voluntariamente de uno o de todos ellos. Si ya tiene una Cuenta de AWS existente con GuardDuty habilitado, puede elegir habilitar cualquiera o todos los planes de protección disponibles en la región. Para obtener información general sobre los planes de protección y qué planes de protección se habilitarán de forma predeterminada, consulte [Precios en GuardDuty](#).

Al habilitar GuardDuty, tenga en cuenta lo siguiente:

- GuardDuty es un servicio regional, lo que significa que cualquiera de los procedimientos de configuración que siga en esta página debe repetirse en cada región que desee supervisar con ayuda de GuardDuty.

Se recomienda que habilite GuardDuty en todas las regiones de AWS compatibles. Esto permite a GuardDuty generar resultados sobre la actividad no autorizada o inusual incluso en las regiones que no utiliza de forma activa. Esto también permite a GuardDuty supervisar los eventos de AWS CloudTrail de los servicios globales de AWS, como IAM. Si GuardDuty no está habilitado en todas las regiones admitidas, se reduce su capacidad para detectar la actividad que involucra servicios globales. Para obtener una lista de las regiones en las que GuardDuty está disponible, consulte [Regiones y puntos de conexión](#).

- Cualquier usuario con privilegios de administrador en una cuenta de AWS puede habilitar GuardDuty; sin embargo, según la práctica recomendada de seguridad de privilegios mínimos, se recomienda crear un rol de IAM, usuario o grupo para administrar GuardDuty de manera específica. Para más información acerca de los permisos necesarios para habilitar GuardDuty, consulte [Permisos necesarios para habilitar GuardDuty](#).
- Al habilitar GuardDuty por primera vez en cualquier Región de AWS, de forma predeterminada, también se habilitan todos los tipos de protección disponibles que se admiten en esa región, incluida Malware Protection for EC2. GuardDuty crea un rol vinculado a un servicio para su

cuenta denominado `AWSServiceRoleForAmazonGuardDuty`. Este rol incluye los permisos y las políticas de confianza que permiten a GuardDuty consumir y analizar eventos directamente desde los [Orígenes de datos fundamentales de GuardDuty](#) para generar resultados de seguridad. Malware Protection for EC2 crea otro rol vinculado al servicio para la cuenta denominado `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Este rol incluye los permisos y políticas de confianza que permiten a Malware Protection for EC2 realizar análisis sin agentes para detectar malware en la cuenta de GuardDuty. Permite a GuardDuty crear una instantánea del volumen de EBS en su cuenta y compartirla con la cuenta de servicio de GuardDuty. Para obtener más información, consulte [Permisos de roles vinculados a servicios de GuardDuty](#). Para más información acerca de los roles vinculados a un servicio, consulte [Uso de roles vinculados a servicios](#).

- Cuando habilita GuardDuty por primera vez en cualquier región, su cuenta de AWS se inscribirá automáticamente en una prueba gratuita de GuardDuty de 30 días en esa región.

En el siguiente video se explica como una cuenta de administrador puede comenzar a utilizar GuardDuty y habilitarlo en múltiples cuentas de miembro.

[Introducción: habilitar Amazon GuardDuty para entornos autónomos o de varias cuentas](#)

Paso 1: habilitación de Amazon GuardDuty

El primer paso para utilizar GuardDuty es habilitarlo en su cuenta. Una vez activado, GuardDuty comenzará inmediatamente a supervisar las amenazas de seguridad en la región actual.

Si desea administrar los resultados de GuardDuty en otras cuentas dentro de su organización como administrador de GuardDuty, debe agregar las cuentas de miembro y habilitar GuardDuty también para ellos.

Note

Si desea habilitar la protección contra malware para S3 de GuardDuty sin habilitar GuardDuty, consulte los pasos a seguir en [Protección contra malware para S3 de GuardDuty](#).

Standalone account environment

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>
2. Seleccione la opción Amazon GuardDuty: todas las características.
3. Elija Comenzar.
4. Consulte las condiciones del servicio en la página Bienvenido a GuardDuty. Elija Enable GuardDuty (Habilitar GuardDuty).

Multi-account environment

Important

Como requisitos previos para este proceso, debe estar en la misma organización que todas las cuentas que desee administrar y tener acceso a la cuenta de administración de AWS Organizations para delegar un administrador para GuardDuty en su organización. Es posible que se necesiten permisos adicionales para delegar un administrador. Para más información, consulte [Permisos necesarios para designar una cuenta de administrador delegado de GuardDuty](#).

Para designar una cuenta de administrador delegado de GuardDuty

1. Abra la consola de AWS Organizations en <https://console.aws.amazon.com/organizations/> mediante la cuenta de administración.
2. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

¿GuardDuty ya está habilitado en la cuenta?

- Si GuardDuty aún no se ha activado, seleccione Comenzar y, a continuación, designe un administrador delegado de GuardDuty en la página de Bienvenido a GuardDuty.
 - Si GuardDuty está habilitado, puede designar un administrador delegado del servicio en la página Configuración.
3. Introduzca los doce dígitos del ID de cuenta de AWS correspondiente a la cuenta que desea designar como administrador delegado de GuardDuty en la organización y seleccione Delegar.

Note

Si GuardDuty aún no está habilitado, cuando se designe un administrador delegado, el servicio se habilitará para esa cuenta en la región actual.

Agregación de cuentas de miembro

Este procedimiento cubre la agregación de cuentas de miembro a una cuenta de administrador delegado de GuardDuty mediante AWS Organizations. También existe la opción de agregar miembros mediante invitación. Para obtener más información sobre ambos métodos para asociar miembros en GuardDuty, consulte [Múltiples cuentas en Amazon GuardDuty](#).

1. Inicie sesión en la cuenta de administrado delegado
2. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
3. En el panel de navegación, elija Settings (Configuración) y Accounts (Cuentas).

En la tabla de cuentas aparecen todas las cuentas de la organización.

4. Para elegir las cuentas que desea agregar como miembros, seleccione la casilla situada junto al ID de la cuenta. A continuación, en el menú Acción, seleccione Agregar miembro.

Tip

Puede automatizar la adición de nuevas cuentas como miembros activando la característica Habilitación automática; sin embargo, esto solo se aplica a las cuentas que se unen a su organización una vez habilitada la característica.

Paso 2: generación de resultados de muestra y exploración de las operaciones básicas

Cuando GuardDuty descubre un problema de seguridad, genera un resultado. Un resultado de GuardDuty es un conjunto de datos que contiene detalles relacionados con ese problema de seguridad único. Los detalles del resultado se pueden utilizar para ayudarle a investigar el problema.

GuardDuty permite generar resultados de muestra con valores de marcador de posición, que se pueden utilizar para probar la funcionalidad de GuardDuty y familiarizarse con los resultados

antes de tener que responder a un problema de seguridad real descubierto por GuardDuty. Siga la guía que aparece a continuación para generar resultados de muestra para cada tipo de resultado disponible en GuardDuty. Para ver otras formas de generar resultados de muestra, incluida la generación de un evento de seguridad simulado en su cuenta, consulte [Hallazgos de ejemplo](#).

Creación y exploración de los resultados de muestra

1. En el panel de navegación, seleccione Configuración.
2. En la página Settings, en Sample findings, elija Generate sample findings.
3. En el panel de navegación, seleccione Resumen para ver la información sobre los resultados generados en su entorno de AWS. Para obtener más información acerca de los componentes del panel de resumen, consulte [Panel de resumen en Amazon GuardDuty](#).
4. En el panel de navegación, seleccione Resultados. Los resultados de muestra se muestran en la página Resultados actuales con el prefijo [SAMPLE].
5. Seleccione un resultado de la lista para ver sus detalles.
 - Puede revisar los distintos campos de información disponibles en el panel de detalles del resultado. Los distintos tipos de resultados pueden tener campos diferentes. Para obtener más información acerca de los campos disponibles en todos los tipos de resultados, consulte [Detalles de los resultados](#). Puede llevar a cabo las siguientes acciones en el panel de detalles:
 - Seleccione el ID de resultado en la parte superior del panel para abrir los detalles JSON completos del resultado. El archivo JSON completo también se puede descargar desde este panel. El JSON contiene información adicional que no se incluye en la vista de consola y es el formato que pueden incorporar otras herramientas y servicios.
 - Consulte la sección Recurso afectado. Si se trata de un resultado real, la información que aparece aquí le ayudará a identificar un recurso de su cuenta que debería investigarse e incluirá enlaces a la Consola de administración de AWS adecuada para consultar recursos procesables.
 - Seleccione los iconos de la lupa con el signo + o - para crear un filtro inclusivo o exclusivo para ese detalle. Para obtener más información acerca de los filtros de resultados, consulte [Filtrado de resultados en GuardDuty](#).
6. Archivado de todos los resultados de muestra
 - a. Para seleccionar todos los resultados, marque la casilla de verificación situada en la parte superior de la lista.

- b. Anule la selección de los resultados que desee conservar.
- c. Seleccione el menú Acciones y, a continuación, seleccione Archivar para ocultar los resultados de muestra.

 Note

Para ver los resultados archivados, seleccione Actual y, a continuación, Archivado para cambiar la vista de los resultados.

Paso 3: configuración de la exportación de los resultados de GuardDuty a un bucket de Amazon S3

GuardDuty recomienda configurar los ajustes para exportar los resultados, ya que le permiten exportar los resultados a un bucket de S3 para su almacenamiento indefinido más allá del periodo de retención de 90 días de GuardDuty. Esto le permite mantener un registro de los resultados o hacer un seguimiento de los problemas en su entorno de AWS a lo largo del tiempo. GuardDuty cifra los datos de los resultados en el bucket S3 mediante el uso de AWS Key Management Service (AWS KMS key). Para configurar los ajustes, deberá dar permiso a GuardDuty para utilizar una clave de KMS. Para ver más pasos detallados, consulte [Exportar los resultados generados a Amazon S3](#).

Para exportar los resultados de GuardDuty a buckets de Amazon S3

1. Adjunte la política a la clave de KMS
 - a. Inicie sesión en la Consola de administración de AWS y abra la consola AWS Key Management Service (AWS KMS) en <https://console.aws.amazon.com/kms>.
 - b. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
 - c. En el panel de navegación, elija Claves administradas por el cliente.
 - d. Seleccione una clave de KMS existente o siga los pasos para [crear una clave de KMS de cifrado simétrico](#) que se indican en la Guía para desarrolladores de AWS Key Management Service.

La región de su clave de KMS y de su bucket de Amazon S3 debe ser la misma.

Copie la clave de ARN en un bloc de notas para utilizarla en los pasos posteriores.

- e. En la sección Política de claves, elija Editar. Si aparece Cambiar a vista de política, elíjala para mostrar la Política de claves y, a continuación, elija Editar.
- f. Copie el siguiente bloque de política en la política de clave de 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"
    }
  }
}
```

Para editar la política, sustituya los siguientes valores formateados en *rojo* en el ejemplo de la política:

1. Sustituya el *ARN de la clave de KMS* por el nombre de recurso de Amazon (ARN) de la clave de KMS. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service.
2. Sustituya *123456789012* por el ID de Cuenta de AWS que posee la cuenta de GuardDuty que exporta los resultados.
3. Sustituya *Region2* por la Región de AWS donde se generan los resultados de GuardDuty.
4. Sustituya *SourceDetectorID* por el detectorID de la cuenta de GuardDuty en la región específica donde se generaron los resultados.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

2. Asociar la política al bucket de Amazon S3

Si aún no dispone de un bucket de Amazon S3 al que desee exportar estos resultados, consulte [Crear un bucket](#) en la Guía del usuario de Amazon S3.

- a. Siga los pasos descritos en [Para crear o editar una política de bucket](#) en la Guía del usuario de Amazon S3, hasta que aparezca la página Editar política de bucket.
- b. La política de ejemplo muestra cómo conceder a GuardDuty permiso para exportar resultados al bucket de Amazon S3. Si cambia la ruta después de configurar la exportación de resultados, deberá modificar la política para conceder permiso a la nueva ubicación.

Copie la siguiente política de ejemplo y péguela en el Editor de políticas de bucket.

Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de la política de la clave de KMS es válida.

Política de ejemplo de bucket de S

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. Para editar la política, sustituya los siguientes valores formateados en *rojo* en el ejemplo de la política:
1. Sustituya el *ARN del bucket de Amazon S3* por el nombre de recurso de Amazon (ARN) del bucket de Amazon S3. Encontrará el ARN del bucket en la página Editar política de bucket de la consola <https://console.aws.amazon.com/s3/>.
 2. Sustituya *123456789012* por el ID de Cuenta de AWS que posee la cuenta de GuardDuty que exporta los resultados.
 3. Sustituya *Region2* por la Región de AWS donde se generan los resultados de GuardDuty.
 4. Sustituya *SourceDetectorID* por el detectorID de la cuenta de GuardDuty en la región específica donde se generaron los resultados.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

5. Sustituya la parte *[prefijo opcional]* del valor del marcador de posición *ARN/[prefijo opcional] del bucket de S3* por una ubicación de carpeta opcional

a la que desee exportar los resultados. Para obtener más información sobre el uso de prefijos, consulte [Organizar objetos mediante prefijos](#) en la Guía del usuario de Amazon S3.

Al proporcionar una ubicación de carpeta opcional que aún no existe, GuardDuty creará esa ubicación solamente si la cuenta asociada al bucket de S3 es la misma que la cuenta que exporta los resultados. Al exportar resultados a un bucket de S3 que pertenece a otra cuenta, la ubicación de la carpeta ya debe existir.

6. Sustituye el *ARN de la clave de KMS* por el nombre de recurso de Amazon (ARN) de la clave de KMS asociada al cifrado de los resultados exportados al bucket de S3. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service.

3. Pasos en la consola de GuardDuty

- a. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
- b. En el panel de navegación, seleccione Configuración.
- c. En la página Configuración, bajo Opciones de exportación de resultados, en Bucket de S3, elija Configurar ahora (o Editar, según sea necesario).
- d. Para el ARN del bucket S3, introduzca el lugar **bucket ARN** al que desea enviar los resultados. Para ver el ARN del bucket, consulte [Ver las propiedades de un bucket de S3](#) en la Guía del usuario de Amazon S3.
- e. En ARN de la clave de KMS, ingrese el **key ARN**. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service.
- f. Seleccione Save.

Paso 4: configuración de alertas de resultados de GuardDuty a través de SNS

GuardDuty se integra con Amazon EventBridge, que se puede utilizar para enviar los datos de los resultados a otras aplicaciones y servicios para su procesamiento. Con EventBridge, puede utilizar los resultados de GuardDuty para iniciar respuestas automáticas a sus resultados. Para ello, conecte los eventos de resultados con destinos como las funciones de AWS Lambda, la automatización de Systems Manager en Amazon EC2, Amazon Simple Notification Service (SNS), etc.

En este ejemplo, creará un tema de SNS para que sea el destino de una regla de EventBridge y, a continuación, utilizará EventBridge para crear una regla que capture los datos de los resultados de GuardDuty. La regla resultante reenvía los detalles de los resultados a una dirección de correo electrónico. Para obtener información sobre cómo enviar resultados a Slack o Amazon Chime y cómo modificar los tipos de resultados por los que se envían las alertas, consulte [Configuración de un punto de conexión y un tema de Amazon SNS](#).

Creación de un tema de SNS para sus alertas de resultados

1. Abra la consola de Amazon SNS en <https://console.aws.amazon.com/sns/v3/home>.
2. En el panel de navegación, elija Temas.
3. Elija Create Topic (Crear tema).
4. En Tipo, seleccione Estándar.
5. En Nombre, escriba **GuardDuty**.
6. Elija Create Topic (Crear tema). Se abrirán los detalles del nuevo tema.
7. En la sección Suscripciones, elija Crear suscripción.
8. En Protocolo, elige Correo electrónico.
9. En Punto de conexión, introduzca la dirección de correo electrónico a la que desea enviar notificaciones.
10. Elija Crear suscripción.

Después de crear su suscripción, debe confirmarla a través de su dirección de correo electrónico.

11. Para comprobar si hay un mensaje de suscripción, vaya a la bandeja de entrada de su correo electrónico y, en el mensaje de suscripción, seleccione Confirmar suscripción.

Note

Para comprobar el estado de la confirmación de correo electrónico, vaya a la consola de SNS y seleccione Suscripciones.

Para crear una regla de EventBridge para capturar resultados de GuardDuty y darles formato

1. Abra la consola de EventBridge en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, seleccione Reglas.

3. Elija Creación de regla.
4. Escriba un nombre y una descripción para la regla.

Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

5. En Bus de eventos, elija Predeterminado.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Seleccione Siguiente.
8. En Origen de eventos, seleccione (Eventos de AWS).
9. En la sección Patrón de eventos, seleccione Formulario de patrón de eventos.
10. En Origen de evento, seleccione Servicios de AWS.
11. En Servicio de AWS, elija GuardDuty.
12. En Tipo de evento, elija Resultado de GuardDuty.
13. Elija Siguiente.
14. En Tipos de destino, seleccione Servicio de AWS.
15. En Seleccionar un destino, elija Tema de SNS y, en Tema, elija el nombre del tema de SNS que creó anteriormente.
16. En la sección Additional settings, en Configurar la entrada de destino, elija Transformador de entrada.

Al agregar un transformador de entrada, se da un formato a los datos de resultados de JSON enviados desde GuardDuty que los convierte en un mensaje legible para las personas.

17. Elija Configurar transformador de entrada.
18. En la sección Transformador de entrada de destino, en Ruta de entrada, pegue el siguiente código:

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

19. Para formatear el correo electrónico, en Plantilla, pegue el siguiente código y asegúrese de sustituir el texto que aparece en rojo por los valores que correspondan a la región:

```
"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. Seleccione Confirmar.
21. Elija Siguiente.
22. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulte [Etiquetas de Amazon EventBridge](#) en la Guía del usuario de Amazon EventBridge.
23. Elija Siguiente.
24. Revise los detalles de la regla y seleccione Creación de regla.
25. (Opcional) Pruebe la nueva regla generando resultados de muestra con el proceso descrito en el paso 2. Recibirá un correo electrónico por cada resultado de muestra que se genere.

Pasos a seguir a continuación

A medida que siga utilizando GuardDuty, comprenderá los tipos de resultados que son relevantes para su entorno. Cada vez que reciba un nuevo resultado, podrá encontrar información, como recomendaciones para corregir dicho resultado, al seleccionar Más información en la descripción del resultado en el panel de detalles del resultado o al buscar el nombre del resultado en [Tipos de resultados de GuardDuty](#).

Las siguientes características le ayudarán a ajustar GuardDuty para que pueda proporcionar los resultados más relevantes para su entorno de AWS:

- Para ordenar fácilmente los resultados en función de criterios específicos, como el ID de instancia, el ID de cuenta, el nombre del bucket de S3, etc., puede crear y guardar filtros en GuardDuty. Para obtener más información, consulte [Filtrado de resultados en GuardDuty](#).
- Si recibe resultados sobre el comportamiento esperado de su entorno, puede archivarlos automáticamente en función de los criterios que defina con las [reglas de supresión](#).

- Para evitar que se generen resultados a partir de un subconjunto de IP confiables, o para que GuardDuty supervise las IP fuera de su alcance de supervisión normal, puede configurar [listas de IP confiables y de amenazas](#).

Orígenes de datos fundamentales de GuardDuty

GuardDuty utiliza los orígenes de datos fundamentales para detectar la comunicación con dominios y direcciones IP maliciosos conocidos, e identificar comportamientos potencialmente anómalos y actividades no autorizadas. Mientras se transfieren de estos orígenes de datos a GuardDuty, todos los datos de registro están cifrados. GuardDuty extrae varios campos de estos orígenes de registro para la generación de perfiles y la detección de anomalías, y, a continuación, descarta los registros.

Al habilitar GuardDuty por primera vez en una región, se ofrece una prueba gratuita de 30 días que incluye la detección de amenazas para todos los orígenes de datos fundamentales. Durante esta prueba gratuita, podrá supervisar un uso mensual estimado desglosado por cada origen de datos fundamental. Como cuenta administradora delegado de GuardDuty, puede ver el costo estimado de uso mensual desglosado por cada cuenta de miembro que pertenece a la organización y que tenga habilitado GuardDuty. Una vez finalizados los 30 días de prueba, podrá utilizar AWS Billing para obtener información sobre el costo de uso.

No hay costo adicional cuando GuardDuty accede a los eventos y registros de estos orígenes de datos fundamentales.

Después de habilitar GuardDuty en la Cuenta de AWS, automáticamente comenzará a supervisar los orígenes de registro que se explican en las siguientes secciones. No necesita habilitar nada más para que GuardDuty comience a analizar y procesar estos orígenes de datos para generar resultados de seguridad asociados.

Temas

- [Eventos de administración de AWS CloudTrail](#)
- [Logs de flujo de VPC](#)
- [Registros de consultas de DNS de Route53 Resolver](#)

Eventos de administración de AWS CloudTrail

AWS CloudTrail le proporciona un historial de las llamadas a la API de AWS de su cuenta, incluidas las llamadas a la API hechas mediante la Consola de administración de AWS, los AWS SDK, las herramientas de línea de comandos y determinados servicios de AWS. CloudTrail también le ayuda a identificar qué usuarios y cuentas invocaron las API de AWS para los servicios compatibles con CloudTrail, la dirección IP de origen desde el que se invocaron las llamadas y el momento en que

estas se invocaron. Para obtener más información, consulte [What is AWS CloudTrail](#) en la Guía del usuario de AWS CloudTrail.

GuardDuty supervisa los eventos de administración de CloudTrail, también conocidos como eventos del plano de control. Estos eventos proporcionan información sobre las operaciones de administración que se realizan en los recursos en la Cuenta de AWS.

A continuación, se incluyen ejemplos de eventos de administración de CloudTrail que GuardDuty supervisa:

- Configuración de la seguridad (operaciones de la API `AttachRolePolicy` de IAM)
- Configuración de reglas para el direccionamiento de datos (operaciones de la API `CreateSubnet` de Amazon EC2)
- Configuración de registros (operaciones de la API `CreateTrail` de AWS CloudTrail)

Cuando habilita GuardDuty, comienza a consumir los eventos de administración de CloudTrail directamente desde CloudTrail a través de un flujo de eventos independiente y duplicado, y analiza sus registros de eventos de CloudTrail.

GuardDuty no administra los eventos de CloudTrail ni afecta a las configuraciones de CloudTrail existentes. Del mismo modo, las configuraciones de CloudTrail no afectan a la forma en que GuardDuty consume y procesa los registros de eventos. Para administrar el acceso y la retención de sus eventos de CloudTrail, utilice la API o la consola del servicio de CloudTrail. Para más información, consulte [Viewing events with CloudTrail event history](#) en la Guía del usuario de AWS CloudTrail.

Cómo administra GuardDuty los eventos globales de AWS CloudTrail

Para la mayoría de los servicios de AWS, los eventos de CloudTrail se registran en la Región de AWS donde se crearon. En el caso de servicios globales como AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon CloudFront y Amazon Route 53 (Route 53), los eventos solo se generan en la región en la que se producen, pero tienen una importancia global.

Cuando GuardDuty consume [eventos del servicio global](#) (GSE) de CloudTrail con valor de seguridad como configuraciones de red o permisos de usuario, replica esos eventos y los procesa en cada región en la que haya activado GuardDuty. Este comportamiento ayuda a GuardDuty a mantener los perfiles de usuario y de rol en cada región, lo cual es vital para detectar eventos anómalos.

 Note

En el caso de los resultados generados a partir de estos eventos de servicio globales, el valor de región del resultado puede diferir del de la región en la que GuardDuty crea la detección. Por ejemplo, un resultado podría mostrar us-east-1 como la región incluso si GuardDuty crea la detección en una región diferente.

Se recomienda que habilite GuardDuty en todas las Regiones de AWS disponibles en su Cuenta de AWS, Incluso si no tiene recursos implementados en determinadas regiones, habilitar GuardDuty ayuda a proteger la cuenta de posibles amenazas. Los actores de amenazas pueden lanzar ataques a través de servicios globales (como IAM, AWS STS o Amazon CloudFront). Pueden intentar crear recursos no autorizados para explotar las regiones en las que su presencia es limitada. GuardDuty procesa los eventos de servicio globales en todas las regiones en las que ha activado el servicio, incluidas las regiones predeterminadas y opcionales. Esto ayuda a GuardDuty a detectar actividades potencialmente sospechosas en las Cuenta de AWS, incluidas las regiones en las que no utiliza recursos de forma activa.

Logs de flujo de VPC

La característica de registros de flujo de la VPC de Amazon VPC captura información acerca del tráfico IP entrante y saliente de las interfaces de red asociadas a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de su entorno de AWS.

Cuando habilita GuardDuty, comienza a analizar inmediatamente los registros de flujo de la VPC de las instancias de Amazon EC2 dentro de su cuenta. Consume eventos de registro de flujo de VPC directamente desde la característica Registros de flujo de VPC a través de una secuencia independiente y duplicada de registros de flujo. Este proceso no afecta a ninguna configuración de los registros de flujo existentes.

[Protección de Lambda](#)

La protección de Lambda es una mejora opcional de Amazon GuardDuty. En la actualidad, la supervisión de la actividad de la red de Lambda en GuardDuty incluye los registros de flujo de Amazon VPC de todas las funciones de Lambda de su cuenta, incluso los registros que no utilizan redes de VPC. Para proteger su función de Lambda de posibles amenazas de seguridad, tendrá que configurar la protección de Lambda en su cuenta de GuardDuty. Para obtener más información, consulte [Protección de Lambda](#).

Supervisión del tiempo de ejecución de GuardDuty

Al administrar el agente de seguridad (ya sea manualmente o a través de GuardDuty) en la supervisión en tiempo de ejecución de EKS o en la supervisión en tiempo de ejecución para instancias de EC2, y GuardDuty se encuentre actualmente implementado en una instancia de Amazon EC2 y recibe el [Tipos de eventos de tiempo de ejecución recopilados](#) de esta instancia, GuardDuty no cobrará a la Cuenta de AWS por el análisis de los registros de flujo de la VPC procedentes de esta instancia de Amazon EC2. Esto ayuda a GuardDuty a evitar el doble costo de uso en la cuenta.

GuardDuty no administra los registros de flujo ni los hace accesibles en la cuenta. Para administrar el acceso y la retención de los registros de flujo, debe configurar la característica Registros de flujo de VPC.

Registros de consultas de DNS de Route53 Resolver

Si utiliza resolvers de DNS de AWS para las instancias de Amazon EC2 (la configuración predeterminada), GuardDuty podrá acceder y procesar los registros de consultas de DNS de Route53 Resolver de solicitud y respuesta a través de los resolvers de DNS internos de AWS. Si utiliza otro solucionador de DNS, como OpenDNS o GoogleDNS, o si configura sus propios solucionadores de DNS, GuardDuty no puede acceder a datos de este origen de datos ni procesarlos.

Al habilitar GuardDuty, comienza inmediatamente a analizar los registros de consultas de DNS de Route53 Resolver a partir de una secuencia de datos independiente. Este flujo de datos es independiente de los datos proporcionados a través de la característica [Registro de consultas del solucionador de Route 53](#). La configuración de esta característica no afecta al análisis de GuardDuty.

Note

GuardDuty no admite la supervisión de registros de DNS para instancias de Amazon EC2 que se lanzan en AWS Outposts porque la característica de registro de consultas de Amazon Route 53 Resolver no está disponible en ese entorno.

Detección Extendida de Amenazas de GuardDuty

La Detección Extendida de Amenazas GuardDuty detecta automáticamente los ataques en varias etapas que abarcan fuentes de datos, varios tipos de recursos de AWS y tiempo, en una Cuenta de AWS. Con esta capacidad, GuardDuty se centra en la secuencia de varios eventos que observa mediante la supervisión de diferentes tipos de orígenes de datos. La Detección Extendida de Amenazas correlaciona estos eventos para identificar los escenarios que se presentan como una amenaza potencial para su entorno de AWS y, a continuación, genera resultados de la secuencia de ataque.

Temas

- [Ejemplos de escenarios de amenazas en la secuencia de ataque](#)
- [Funcionamiento](#)
- [Habilitar planes de protección para maximizar la detección de amenazas](#)
- [Detección extendida de amenazas en la consola de GuardDuty](#)
- [Descripción y administración de resultados de secuencias de ataques](#)
- [Recursos adicionales](#)

Ejemplos de escenarios de amenazas en la secuencia de ataque

La Detección Extendida de Amenazas cubre los escenarios de amenazas que implican compromisos relacionados con el uso indebido de credenciales de AWS, intentos de comprometer datos en buckets de Amazon S3 y comprometer recursos de contenedores y Kubernetes en clústeres de Amazon EKS. Un único resultado puede abarcar una secuencia de ataque completa. Por ejemplo, en la siguiente lista se describen los escenarios que GuardDuty puede detectar:

Ejemplo 1: las credenciales de AWS y los datos del bucket de Amazon S3 están comprometidos

- Un actor de amenazas que obtiene acceso no autorizado a una carga de trabajo informática.
- Luego, el actor realiza una serie de acciones, como aumentar los privilegios y establecer la persistencia.
- Por último, el actor que extrae datos de un recurso de Amazon S3.

Ejemplo 2: Compromiso con el clúster de Amazon EKS

- Un actor de amenazas intenta explotar una aplicación contenedora dentro de un clúster de Amazon EKS.

- El actor usa ese contenedor comprometido para obtener tokens de cuentas de servicio privilegiadas.
- Luego, el actor aprovecha estos privilegios elevados para acceder a secretos de Kubernetes o recursos de AWS confidenciales a través de las identidades de los pods.

Debido a la naturaleza de los escenarios de amenaza asociados, GuardDuty considera todos los [Tipos de resultados de secuencias de ataque](#) como Críticos.

En el siguiente vídeo se muestra cómo utilizar la Detección Extendida de Amenazas.

[Demostración de la Detección Extendida de Amenazas de Amazon GuardDuty](#)

Funcionamiento

Cuando se habilita Amazon GuardDuty en su cuenta en una Región de AWS específica, la Detección Extendida de Amenazas también está habilitada de forma predeterminada. El uso de Detección Extendida de Amenazas no conlleva ningún costo adicional. De forma predeterminada, correlaciona los eventos en todos los [Orígenes de datos fundamentales](#). Sin embargo, si se habilitan más planes de protección de GuardDuty, como S3 Protection, EKS Protection y Runtime Monitoring, se abrirán tipos adicionales de detecciones de secuencias de ataques al ampliar la gama de fuentes de eventos. Esto podría ayudar a realizar un análisis de amenazas más exhaustivo y a detectar mejor las secuencias de ataque. Para obtener más información, consulte [Habilitar planes de protección para maximizar la detección de amenazas](#).

GuardDuty correlaciona varios eventos, incluidas las actividades de la API y los resultados de GuardDuty. Estos eventos se denominan señales. A veces, es posible que se produzcan eventos en su entorno que, por sí solos, no se presenten como una amenaza potencial clara. GuardDuty las denomina señales débiles. Con la Detección Extendida de Amenazas, GuardDuty identifica cuándo una secuencia de varias acciones se alinea con una actividad potencialmente sospechosa y genera un resultado de secuencia de ataque en su cuenta. Estas múltiples acciones pueden incluir señales débiles y resultados de GuardDuty ya identificados en su cuenta.

Note

Al correlacionar los eventos con las secuencias de ataque, la Detección Extendida de Amenazas no tiene en cuenta las conclusiones archivadas, incluidas las que se archivan

automáticamente debido a [Reglas de supresión](#). Este comportamiento garantiza que solo las señales activas y relevantes contribuyan a la detección de la secuencia de ataque. Para asegurarse de que esto no lo afecte, consulte las normas de supresión vigentes en su cuenta. Para obtener más información, consulte [Uso de reglas de supresión con Detección Extendida de Amenazas](#).

GuardDuty también está diseñado para identificar posibles comportamientos de ataque recientes o en curso (dentro de un período de 24 horas) en su cuenta. Por ejemplo, un ataque podría comenzar cuando un actor accede involuntariamente a una carga de trabajo de cómputo. Luego, el actor realizaría una serie de pasos, como la enumeración, el aumento de privilegios y la exfiltración de credenciales de AWS. Estas credenciales podrían utilizarse para comprometer aún más los datos o acceder de forma malintencionada a ellos.

Habilitar planes de protección para maximizar la detección de amenazas

Para cualquier cuenta de GuardDuty de una región, la función de Detección Extendida de Amenazas se activa automáticamente. De forma predeterminada, esta capacidad tiene en cuenta los múltiples eventos de todas las [Orígenes de datos fundamentales](#). Para beneficiarse de esta capacidad, no es necesario activar todos los [planes de protección GuardDuty centrados en los casos de uso](#). Por ejemplo, con la detección de amenazas básica, GuardDuty puede identificar una posible secuencia de ataque a partir de la actividad de descubrimiento de privilegios de IAM en las API de Amazon S3 y detectar las alteraciones posteriores en el plano de control de S3, como los cambios que hacen que la política de recursos de bucket sea más permisiva.

La Detección Extendida de Amenazas está diseñada de tal manera que, si habilita más planes de protección, ayuda a GuardDuty a correlacionar señales más diversas en múltiples orígenes de datos. Esto podría aumentar la amplitud de las señales de seguridad para un análisis exhaustivo de las amenazas y la cobertura de las secuencias de ataque. Para identificar los resultados que podrían ser una de las múltiples etapas de una secuencia de ataque, GuardDuty recomienda habilitar planes de protección específicos: S3 Protection, EKS Protection y Runtime Monitoring (con el complemento EKS).

Temas

- [Detección de secuencias de ataque en clústeres de Amazon EKS](#)

- [Detección de secuencias de ataques en los buckets de Amazon S3](#)

Detección de secuencias de ataque en clústeres de Amazon EKS

GuardDuty correlacionó varias señales de seguridad en los registros de auditoría de EKS, el comportamiento de los procesos en tiempo de ejecución y la actividad de la API de AWS para detectar patrones de ataque sofisticados. Para beneficiarse de la Detección Extendida de Amenazas para EKS, debe habilitar al menos una de estas funciones: EKS Protection o el monitoreo del tiempo de ejecución (con el complemento EKS). EKS Protection supervisa las actividades del plano de control mediante registros de auditoría, mientras que Runtime Monitoring observa los comportamientos dentro de los contenedores.

Para obtener la máxima cobertura y una detección integral de amenazas, GuardDuty recomienda habilitar ambos planes de protección. En conjunto, crean una vista completa de sus clústeres de EKS, lo que permite a GuardDuty detectar patrones de ataque complejos. Por ejemplo, puede identificar una implementación anómala de un contenedor privilegiado (detectado con EKS Protection), seguido de intentos de persistencia, minería de criptomonedas y creación de intérpretes de comandos inversos dentro de ese contenedor (detectados con Runtime Monitoring). GuardDuty representa estos eventos relacionados como un único resultado de gravedad crítica, denominado [AttackSequence:EKS/CompromisedCluster](#). Al activar ambos planes de protección, los resultados de la secuencia de ataque abarca los siguientes escenarios de amenaza:

- Compromiso de los contenedores que ejecutan aplicaciones web vulnerables
- Acceso no autorizado mediante credenciales mal configuradas
- Intentos de escalar los privilegios
- Solicitudes de la API sospechosas
- Intentos para acceder a los datos de forma malintencionada

La siguiente lista proporciona detalles sobre cuándo se activan estos planes de protección dedicados de forma individual:

EKS Protection

Al habilitar EKS Protection, GuardDuty puede detectar secuencias de ataques que involucren actividades en el plano de control del clúster de Amazon EKS. Esto permite a GuardDuty correlacionar los registros de auditoría de EKS y la actividad de la API de AWS. Por ejemplo, GuardDuty puede detectar una secuencia de ataque en la que un actor intenta acceder sin

autorización a los secretos de un clúster, modifica los permisos del control de acceso basado en roles (RBAC) de Kubernetes y crea grupos privilegiados. Para obtener información sobre cómo habilitar este plan de protección, consulte [EKS Protection](#).

Runtime Monitoring de Amazon EKS

Al habilitar Runtime Monitoring para los clústeres de Amazon EKS, GuardDuty puede mejorar la detección de secuencias de ataques de EKS con visibilidad a nivel de contenedor. Esto ayuda a GuardDuty a detectar posibles procesos maliciosos, comportamientos sospechosos en tiempo de ejecución y posibles ejecuciones de malware. Por ejemplo, GuardDuty puede detectar una secuencia de ataque en la que un contenedor comienza a mostrar un comportamiento sospechoso, como procesos de minería de criptomonedas o establecer conexiones con puntos de conexión maliciosos conocidos. Para obtener información sobre cómo habilitar este plan de protección, consulte [Supervisión en tiempo de ejecución](#).

Si no se habilita la protección fr EKS o Runtime Monitoring, GuardDuty no podrá generar [Tipos de resultados de la protección de EKS](#) individual ni [Tipos de resultados de la supervisión en tiempo de ejecución](#). Por lo tanto, GuardDuty no podrá detectar secuencias de ataque en varias etapas que impliquen resultados asociados.

Detección de secuencias de ataques en los buckets de Amazon S3

Al habilitar la S3 Protection, GuardDuty puede detectar secuencias de ataques que implican intentos de comprometer datos en sus buckets de Amazon S3. Sin la S3 Protection, GuardDuty puede detectar cuándo su política de recursos de bucket de S3 se vuelve demasiado permisiva. Al habilitar la S3 Protection, GuardDuty adquiere la capacidad de detectar posibles actividades de exfiltración de datos que pueden producirse después de que su bucket de S3 se vuelva demasiado permisivo.

Si la S3 Protection no está habilitada, GuardDuty no podrá generar [Tipos de resultados de la S3 Protection](#) individuales. Por lo tanto, GuardDuty no podrá detectar secuencias de ataque en varias etapas que impliquen resultados asociados. Para obtener información sobre cómo habilitar este plan de protección, consulte [Protección de S3](#).

Detección extendida de amenazas en la consola de GuardDuty

De forma predeterminada, la página Detección Extendida de Amenazas de la consola GuardDuty muestra el estado como Activado. Con la detección de amenazas básica, el estado indica que GuardDuty puede detectar una posible secuencia de ataque que implique una actividad de

descubrimiento de privilegios de IAM en las API de Amazon S3 y detectar alteraciones posteriores en el plano de control de S3.

Siga los siguientes pasos para acceder a la página Detección Extendida de Amenazas en la consola GuardDuty:

1. Puede abrir la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación izquierdo, elija Detección Extendida de Amenazas.

Esta página proporciona detalles sobre los escenarios de amenazas que cubre la Detección Extendida de Amenazas.

3. En la página Detección Extendida de Amenazas, consulte la sección Planes de protección relacionados. Si desea habilitar planes de protección dedicados para mejorar la cobertura de detección de amenazas en su cuenta, seleccione la opción Configurar para ese plan de protección.

Descripción y administración de resultados de secuencias de ataques

Los resultados de la secuencia de ataque son como otros resultados de GuardDuty en su cuenta. Puede verlos en la página Resultados en la consola de GuardDuty. Para obtener información sobre cómo ver los resultados, consulte [Página de resultados en la consola de GuardDuty](#).

Al igual que otros resultados de GuardDuty, los resultados de la secuencia de ataque también se envían automáticamente a Amazon EventBridge. Según su configuración, los resultados de la secuencia de ataques también se exportan a un destino de publicación (bucket de Amazon S3). Para establecer un nuevo destino de publicación o actualizar uno existente, consulte [Exportar los resultados generados a Amazon S3](#).

Recursos adicionales

Consulte las siguientes secciones para comprender mejor las secuencias de ataque:

- Tras obtener más información sobre la Detección Extendida de Amenazas y las secuencias de ataque, puede generar ejemplos de tipos de resultados de secuencias de ataque siguiendo los pasos que se indican en [Hallazgos de ejemplo](#).
- Información sobre [Tipos de resultados de secuencias de ataque](#).

- Revise los resultados y explore los detalles de los resultados asociados con [Detalles de los resultados de la secuencia de ataque](#).
- Priorice y aborde los tipos de resultados de secuencias de ataques siguiendo los pasos correspondientes a los recursos afectados asociados en [Corrección de resultados](#).

EKS Protection en GuardDuty

EKS Protection ayuda a detectar posibles riesgos de seguridad en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) en el entorno de AWS. Por ejemplo, ayuda a detectar cuándo un actor no autenticado accede a un clúster de EKS mal configurado e intenta recopilar secretos o credenciales de AWS del clúster. EKS Protection utiliza los registros de auditoría de EKS para analizar las actividades de los usuarios y las aplicaciones.

Al activar EKS Protection, GuardDuty comienza a supervisar sus clústeres de Amazon EKS de manera automática para detectar posibles amenazas de seguridad. GuardDuty utiliza su propia transmisión independiente para recopilar y analizar [Registros de auditoría de EKS en EKS Protection](#); no se requiere ninguna configuración adicional.

Cuando GuardDuty detecta una amenaza potencial basada en la supervisión del registro de auditoría de EKS, genera un resultado de seguridad. Para obtener información sobre los tipos de resultados que GuardDuty puede generar cuando se habilita EKS Protection, consulte [Tipos de resultados de la protección de EKS](#).

Note

Para ver los registros de auditoría de EKS en su cuenta (opcional), puede configurar el registro del plano de control de Amazon EKS para enviar los registros de auditoría a CloudWatch Logs. Esta configuración es independiente de la protección EKS y no es necesaria para la capacidad de supervisión de seguridad de GuardDuty.

Prueba gratuita de 30 días

- Al habilitar GuardDuty en una Cuenta de AWS en una Región de AWS por primera vez, obtendrá una prueba gratuita de 30 días. En este caso, GuardDuty también habilitará EKS Protection, que está incluida en la prueba gratuita de 30 días.
- Si ya utiliza GuardDuty y decide habilitar EKS Protection por primera vez, la cuenta de esta región recibirá una prueba gratuita de 30 días para EKS Protection.
- Puede optar por desactivar EKS Protection en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, GuardDuty no desactivará

automáticamente EKS Protection. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Estimar el costo de uso](#).

Al desactivar EKS Protection, GuardDuty dejará inmediatamente de supervisar y analizar los registros de auditoría de EKS para los recursos de Amazon EKS.

Es posible que EKS Protection no esté disponible en todas las Regiones de AWS en las que GuardDuty está disponible. Para obtener más información, consulte [Disponibilidad de características específicas por región](#).

Note

La Supervisión en tiempo de ejecución de EKS se administra como parte de la Supervisión en tiempo de ejecución. Para obtener más información, consulte [Supervisión del tiempo de ejecución de GuardDuty](#).

Registros de auditoría de EKS en EKS Protection

Los registros de auditoría de EKS capturan las acciones secuenciales del clúster de Amazon EKS, incluidas las actividades de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control. El registro de auditoría es un componente de todos los clústeres de Kubernetes.

Para obtener más información, consulte la sección de [auditorías](#) en la documentación de Kubernetes.

Amazon EKS permite que los registros de auditoría de EKS se ingieran como registros de Amazon CloudWatch a través de la característica de [registro del plano de control de EKS](#). GuardDuty no administra el registro del plano de control de Amazon EKS ni hace que los registros de auditoría de EKS sean accesibles en la cuenta si no los ha habilitado para Amazon EKS. Para administrar el acceso a los registros de auditoría de EKS y su retención, deberá configurar la característica de registro del plano de control de Amazon EKS. Para obtener más información, consulte [Habilitar y deshabilitar registros de plano de control](#) en la Guía del usuario de Amazon EKS.

Habilitar EKS Protection en entornos de varias cuentas

En un entorno de varias cuentas, solo la cuenta del administrador delegado de GuardDuty tiene la opción de habilitar o desactivar la característica de EKS Protection para las cuentas de miembro de

la organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro mediante AWS Organizations. Esta cuenta de administrador delegado de GuardDuty puede elegir habilitar automáticamente EKS Protection para todas las cuentas nuevas a medida que se unen a la organización. Para obtener más información sobre los entornos multicuenta, consulte [Managing multiple accounts in Amazon GuardDuty](#).

Configurar la supervisión del registro de auditoría de EKS para la cuenta de administrador delegado de GuardDuty

Elija el método de acceso que prefiera para configurar la supervisión de registros de auditoría de EKS para la cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija EKS Protection.
3. En la pestaña Configuración, puede ver el estado de la configuración actual de la supervisión de registros de auditoría de EKS en la respectiva sección. Para actualizar la configuración de la cuenta de administrador delegado de GuardDuty, elija Editar en el panel Supervisión del registro de auditoría de EKS.
4. Realice una de las siguientes acciones:

Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las cuentas de GuardDuty activas de su organización de AWS, lo que incluye las nuevas cuentas que se unan a la organización.
- Seleccione Save.

Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de administrador delegado de GuardDuty, elija Configurar cuentas manualmente.
- Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta).
- Seleccione Save.

API/CLI

Ejecute la operación de la API [updateDetector](#) con su propio ID de detector regional y pase el name del objeto features como EKS_AUDIT_LOGS y status como ENABLED o DISABLED.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Para activar o desactivar la Supervisión de registros de auditoría de EKS, puede ejecutar un comando de la AWS CLI. Asegúrese de utilizar el *ID de detector* válido de la cuenta de administrador delegado de GuardDuty.

Note

El siguiente código de ejemplo habilita la supervisión de registros de auditoría de EKS. Asegúrese de sustituir *12abc34d567e8fa901bc2d34e56789f0* por el detector-id de la cuenta de administrador delegado de GuardDuty y *5555555555* por la Cuenta de AWS de la cuenta de administrador delegado de GuardDuty.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Para deshabilitar la supervisión de registros de auditoría de EKS, sustituya ENABLED por DISABLED.

Habilitación automática de la supervisión de registros de auditoría de EKS para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en todas las cuentas de miembros existentes en la organización.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

Mediante la página EKS Protection

1. En el panel de navegación, elija EKS Protection.
2. En la pestaña Configuración, puede ver el estado actual de la supervisión de registros de auditoría de EKS para las cuentas de miembros activos de su organización.

Para actualizar la configuración de la Supervisión de registros de auditoría de EKS, elija Editar.

3. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la supervisión de registros de auditoría de EKS para las cuentas nuevas y existentes de la organización.
4. Seleccione Save.

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Supervisión de registros de auditoría de EKS.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas y desea personalizar la configuración de la Supervisión de registros de auditoría de EKS para cuentas específicas de

su organización, consulte [Activación o desactivación de forma selectiva de la supervisión de registros de auditoría de EKS para las cuentas de miembros](#).

API/CLI

- Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya ENABLED por DISABLED.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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



Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de UnprocessedAccounts vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la Supervisión de registros de auditoría de EKS para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en todas las cuentas de miembros activos existentes en la organización.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

- Inicie sesión con las credenciales de la cuenta de administrador delegado de GuardDuty.
- En el panel de navegación, elija EKS Protection.
- En la página EKS Protection, puede ver el estado actual de la configuración de Análisis de malware iniciado por GuardDuty. En la sección Cuentas de miembros activas, seleccione Acciones.
- En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
- Seleccione Save.

API/CLI

- Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya ENABLED por DISABLED.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la Supervisión de registros de auditoría de EKS para las cuentas de miembros nuevos

Las cuentas de miembro recién creadas deben Activar GuardDuty antes de seleccionar la configuración del análisis de malware iniciado por GuardDuty. Las cuentas de miembros administradas por invitación pueden configurar manualmente el análisis de malware iniciado por GuardDuty en sus cuentas. Para obtener más información, consulte [Step 3 - Accept an invitation](#).

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en las cuentas de miembros nuevos que se unen a la organización.

Console

La cuenta de administrador delegado de GuardDuty puede habilitar la Supervisión de registros de auditoría de EKS para las cuentas de miembro nuevas en una organización a través de las páginas Supervisión de registros de auditoría de EKS o Cuentas.

Habilitación automática de la Supervisión de registros de auditoría de EKS para las cuentas de miembros nuevos

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:
 - Mediante la página EKS Protection:
 1. En el panel de navegación, elija EKS Protection.
 2. En la página EKS Protection, seleccione Editar en Supervisión de registros de auditoría de EKS.
 3. Elija Configurar cuentas manualmente.
 4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, la supervisión de registros de auditoría de EKS se habilite automáticamente para la cuenta. Solo la cuenta de administrador delegado de GuardDuty de la organización puede modificar esta configuración.
 5. Seleccione Save.
 - Mediante la página Cuentas:

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Supervisión de registros de auditoría de EKS.
4. Seleccione Save.

API/CLI

- Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para las cuentas nuevas, ejecute la operación de la API [UpdateOrganizationConfiguration](#) con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo puede habilitar la supervisión de registros de auditoría de EKS para los nuevos miembros que se unan a su organización. También puede pasar una lista de ID de cuentas separadas por un espacio.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Activación o desactivación de forma selectiva de la supervisión de registros de auditoría de EKS para las cuentas de miembros

Elija su método de acceso preferido para activar o desactiva la supervisión de registros de auditoría de EKS en cuentas de miembros selectivas en la organización.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas, revise la columna Supervisión de registros de auditoría de EKS para ver el estado de su cuenta de miembro.

3. Activación o desactivación de la Supervisión de registros de auditoría de EKS

Seleccione una cuenta que desee configurar para la Supervisión de registros de auditoría de EKS. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione Supervisión de registros de auditoría de EKS y, a continuación, elija la opción adecuada.

API/CLI

Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para sus cuentas de miembros, invoque la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.

El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya ENABLED por DISABLED. También puede pasar una lista de ID de cuentas separadas por un espacio.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Habilitar EKS Protection para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en la cuenta de AWS en una región específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a su caso. Para obtener más información sobre la administración de varias cuentas, consulte [Habilitar EKS Protection en entornos de varias cuentas](#).

Después de habilitar EKS Protection, GuardDuty comenzará a supervisar los registros de auditoría de EKS correspondientes a los clústeres de Amazon EKS de la cuenta.

Elija el método de acceso que prefiera para habilitar la Protección EKS en la cuenta independiente.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el selector de Regiones que aparece en la esquina superior derecha, seleccione una región en la que desee habilitar la protección de EKS.
3. En el panel de navegación, elija Protección de EKS.
4. La página de Protección de EKS muestra el estado actual de la protección de EKS en la cuenta. Elija Habilitar para habilitar la protección de EKS.
5. Elija Confirmar para guardar su selección.

API/CLI

- Ejecute la operación de la API [updateDetector](#) mediante el ID de detector regional de la cuenta de administrador delegado de GuardDuty y al transmitir el nombre de objeto de `features` como `EKS_AUDIT_LOGS` y el estado como `ENABLED`.

También puede habilitar EKS Protection mediante la ejecución de un comando de la AWS CLI. Ejecute el siguiente comando y sustituya `12abc34d567e8fa901bc2d34e56789f0` por el ID de detector de la cuenta y `us-east-1` por la región en la que desea habilitar la protección de EKS.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Protección de S3 en GuardDuty

La protección de S3 ayuda a detectar posibles riesgos para la seguridad de los datos, como su filtración y destrucción, en los buckets de Amazon Simple Storage Service (Amazon S3). GuardDuty supervisa los eventos de datos de AWS CloudTrail para Amazon S3, que incluyen operaciones de la API a nivel de objeto para identificar estos riesgos en todos los buckets de Amazon S3 en la cuenta.

Cuando GuardDuty detecta una amenaza potencial según la supervisión de eventos de datos de S3, genera un resultado de seguridad. Para obtener información sobre los tipos de resultados que GuardDuty puede generar cuando se habilita la protección de S3, consulte [Tipos de resultados de S3 Protection de GuardDuty](#).

De forma predeterminada, la detección de amenazas fundamental incluye la supervisión de [Eventos de administración de AWS CloudTrail](#) para identificar posibles amenazas en los recursos de Amazon S3. Este origen de datos es diferente de los eventos de datos de AWS CloudTrail para S3, ya que ambos supervisan diferentes tipos de actividades en el entorno.

Puede habilitar la protección de S3 en una cuenta en cualquier región en la que GuardDuty [admite esta característica](#). Esto ayudará a supervisar los eventos de datos de CloudTrail para S3 en esa cuenta y región. Después de habilitar la protección de S3, GuardDuty será capaz de supervisar plenamente los buckets de Amazon S3 y generar resultados en caso de acceso sospechoso a los datos almacenados en los buckets de S3.

Para utilizar la protección de S3, no es necesario habilitar ni configurar explícitamente el registro de eventos de datos de S3 en AWS CloudTrail.

Prueba gratuita de 30 días

En la siguiente lista se explica cómo funciona la prueba gratuita de 30 días para la cuenta:

- Al habilitar GuardDuty en una Cuenta de AWS en una nueva región por primera vez, obtendrá una prueba gratuita de 30 días. En este caso, GuardDuty también habilitará la protección de S3, que está incluida en la prueba gratuita.
- Si ya utiliza GuardDuty y decide habilitar la protección de S3 por primera vez, la cuenta de esta región recibirá una prueba gratuita de 30 días para la protección de S3.
- Puede optar por desactivar la S3 Protection en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, la protección

de S3 no se desactivará automáticamente. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Estimar el costo de uso de GuardDuty](#).

Eventos de datos de AWS CloudTrail para S3

En los eventos de datos, también conocidos como operaciones del plano de datos, se muestra información sobre las operaciones de recursos llevadas a cabo en un recurso determinado. Suelen ser actividades de gran volumen.

A continuación se incluyen ejemplos de eventos de datos de CloudTrail para S3 que GuardDuty puede supervisar:

- GetObjectOperaciones de la API de
- PutObjectOperaciones de la API de
- ListObjectsOperaciones de la API de
- DeleteObjectOperaciones de la API de

Para obtener más información sobre estas API, consulte la [Referencia de la API de Amazon Simple Storage Service](#).

Cómo GuardDuty utiliza los eventos de datos de CloudTrail para S3

Al habilitar la protección de S3, GuardDuty comenzará a analizar los eventos de datos de CloudTrail para S3 de todos los buckets de S3, y los supervisará en busca de actividad maliciosa y sospechosa. Para obtener más información, consulte [Eventos de administración de AWS CloudTrail](#).

Si un usuario no autenticado accede a un objeto S3, significa que el objeto S3 es de acceso público. Por lo tanto, GuardDuty no procesa tales solicitudes. GuardDuty procesa las solicitudes realizadas a los objetos de S3 mediante el uso de credenciales de IAM (AWS Identity and Access Management) o AWS STS (AWS Security Token Service) válidas.

Nota

Después de habilitar la protección de S3, GuardDuty supervisará los eventos de datos de los buckets de Amazon S3 que residen en la misma región en la que habilitó GuardDuty.

Si desactiva la protección de S3 en la cuenta en una región específica, GuardDuty detendrá la supervisión de eventos de datos de S3 de los datos almacenados en los buckets de S3. GuardDuty dejará de generar tipos de resultados de la protección de S3 para la cuenta en esa región.

GuardDuty utiliza los eventos de datos de CloudTrail para S3 para las secuencias de ataque

[Detección Extendida de Amenazas de GuardDuty](#) detecta secuencias de ataques en varias etapas que abarcan los orígenes de los datos, los recursos de AWS y el cronograma fundamentales de una cuenta. Cuando GuardDuty observa una secuencia de eventos que indica una actividad sospechosa reciente o en curso en su cuenta, GuardDuty genera un resultado de la secuencia de ataque asociada.

De forma predeterminada, al activar GuardDuty, la Detección Extendida de Amenazas también se habilita en su cuenta. Esta capacidad cubre el escenario de amenazas asociado a los eventos de administración de CloudTrail sin costo adicional. Sin embargo, para aprovechar al máximo el potencial de la Detección Extendida de Amenazas, GuardDuty recomienda habilitar S3 Protection para cubrir los escenarios de amenazas asociados a los eventos de datos de CloudTrail para S3.

Después de habilitar la S3 Protection, GuardDuty cubrirá automáticamente los escenarios de amenaza de la secuencia de ataque, como la puesta en peligro o la destrucción de datos, en los que puedan estar involucrados los recursos de Amazon S3.

Habilitar la protección de S3 en entornos de varias cuentas

En un entorno con varias cuentas, solo la cuenta de administrador delegado de GuardDuty tiene la opción de configurar (habilitar o desactivar) la protección de S3 para las cuentas de miembro en su organización de AWS. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro mediante AWS Organizations. La cuenta de administrador delegado de GuardDuty puede optar por habilitar automáticamente la protección de S3 en todas las cuentas, solo en las nuevas cuentas o en ninguna cuenta de la organización. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Habilitar la protección de S3 para la cuenta de administrador delegado de GuardDuty

Elija el método de acceso que prefiera para habilitar la protección de S3 para la cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección de S3.
3. En la página Protección de S3, seleccione Editar.
4. Realice una de las siguientes acciones:

Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las cuentas de GuardDuty activas de su organización de AWS, lo que incluye las nuevas cuentas que se unan a la organización.
- Seleccione Save.

Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de administrador delegado de GuardDuty, elija Configurar cuentas manualmente.
- Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta).
- Seleccione Save.

API/CLI

Ejecute [updateDetector](#) con el ID de detector de la cuenta de administrador delegado de GuardDuty para la región actual y pase el name del objeto de features como S3_DATA_EVENTS y status como ENABLED.

Como alternativa, puede configurar la protección de S3 mediante la AWS Command Line Interface. Ejecute el siguiente comando, y asegúrese de sustituir **12abc34d567e8fa901bc2d34e56789f0** por el ID de detector de la cuenta de administrador delegado de GuardDuty para la región actual.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Habilitación automática de la protección de S3 para todas las cuentas de miembros de la organización

Elija el método de acceso que prefiera para habilitar la protección de S3 para la cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con la cuenta de administrador.

2. Realice una de las siguientes acciones:

Uso de la página Protección de S3

1. En el panel de navegación, elija Protección de S3.
2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la protección de S3 para las cuentas nuevas y existentes de la organización.
3. Seleccione Save.

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Protección de S3.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitar de forma selectiva la S3 Protection en las cuentas de miembro](#).

API/CLI

- Para habilitar la protección de S3 de forma selectiva para las cuentas de miembro, invoque la operación de la API [updateMemberDetectors](#) con el *ID de detector* propio.
- En el siguiente ejemplo se muestra cómo se puede habilitar la protección de S3 para una sola cuenta de miembro. Asegúrese de sustituir *12abc34d567e8fa901bc2d34e56789f0* por el `detector-id` de la cuenta de administrador delegado de GuardDuty, y *111122223333*.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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



Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la S3 Protection para todas las cuentas de miembros activas existentes

Elija su método de acceso preferido para habilitar la S3 Protection en todas las cuentas de miembros activas existentes de la organización.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

- Inicie sesión con las credenciales de la cuenta de administrador delegado de GuardDuty.
- En el panel de navegación, elija S3 Protection.
- En la página S3 Protection, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
- En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
- Elija Confirmar.

API/CLI

- Para habilitar la S3 Protection de forma selectiva para las cuentas de miembro, invoque la operación de la API [updateMemberDetectors](#) con el *ID de detector* propio.
- En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Asegúrese de sustituir *12abc34d567e8fa901bc2d34e56789f0* por el `detector-id` de la cuenta de administrador delegado de GuardDuty, y *111122223333*.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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



Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la S3 Protection para las cuentas de nuevos miembros

Elija su método de acceso preferido para habilitar la S3 Protection para las cuentas nuevas que se unan a la organización.

Console

La cuenta de administrador delegado de GuardDuty puede habilitar las cuentas de miembro nuevas en una organización a través de la consola, desde la página S3 Protection o la página Cuentas.

Habilitación automática de la S3 Protection para las cuentas de nuevos miembros

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

- Uso de la página S3 Protection:

1. En el panel de navegación, elija S3 Protection.
2. En la página S3 Protection, seleccione Editar.
3. Elija Configurar cuentas manualmente.
4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se una a su organización, la S3 Protection se habilitará automáticamente para la cuenta. Solo la cuenta de administrador delegado de GuardDuty de la organización puede modificar esta configuración.
5. Seleccione Save.

- Mediante la página Cuentas:

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las nuevas cuentas en S3 Protection.
4. Seleccione Save.

API/CLI

- Para habilitar la S3 Protection de forma selectiva para las cuentas de miembro, invoque la operación de la API [UpdateOrganizationConfiguration](#) con el *ID de detector* propio.
- En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Establezca las preferencias para habilitar o deshabilitar automáticamente

el plan de protección en esa región para las nuevas cuentas (NEW) que se unan a la organización, todas las cuentas (ALL) o ninguna de las cuentas (NONE) de la organización. Para obtener más información, consulte [autoEnableOrganizationMembers](#). Según sus preferencias, es posible que deba sustituir NEW por ALL o NONE.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitar de forma selectiva la S3 Protection en las cuentas de miembro

Elija el método de acceso que prefiera para habilitar o desactivar de forma selectiva la S3 Protection en las cuentas de miembro.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas, revise la columna S3 Protection para ver el estado de su cuenta de miembro.

3. Para habilitar de forma selectiva la S3 Protection

Seleccione la cuenta para la que desee habilitar la S3 Protection. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione S3Pro y, a continuación, elija la opción adecuada.

API/CLI

Para habilitar la S3 Protection de forma selectiva para las cuentas de miembro, ejecute la operación de la API [updateMemberDetectors](#) con el ID de detector propio. En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Para desactivarlo, sustituya `true` por `false`.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Note

Si utiliza scripts para incorporar nuevas cuentas y desea deshabilitar la S3 Protection en sus nuevas cuentas, puede modificar la operación de la API [createDetector](#) con el objeto `dataSources` opcional, tal y como se describe en este tema.

Habilitar la S3 Protection para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar la protección de S3 en entornos de varias cuentas](#).

Tras habilitar la S3 Protection, GuardDuty comenzará a supervisar los eventos de datos de AWS CloudTrail para los buckets de S3 en la cuenta.

Elija el método de acceso que prefiera para configurar la S3 Protection para una cuenta independiente.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el selector de Regiones que aparece en la esquina superior derecha, seleccione una región en la que desee habilitar la S3 Protection.
3. En el panel de navegación, elija S3 Protection.
4. En la página S3 Protection se indica el estado actual de la S3 Protection de su cuenta. Seleccione Habilitar o Deshabilitar para habilitar o deshabilitar la S3 Protection en cualquier momento.
5. Elija Confirmar para confirmar su selección.

API/CLI

Ejecute [updateDetector](#) con el ID de detector válido para la región actual y transfiera el name del objeto de features como S3_DATA_EVENTS establecido en ENABLED para habilitar la S3 Protection, respectivamente.

Note

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Como alternativa también puede utilizar la AWS Command Line Interface. Para habilitar la S3 Protection, ejecute el siguiente comando y sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar la S3 Protection.

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

Supervisión del tiempo de ejecución de GuardDuty

La supervisión en tiempo de ejecución observa y analiza los eventos a nivel de sistema operativo, red y archivos para ayudar a detectar posibles amenazas en cargas de trabajo específicas del entorno de AWS.

Recursos de AWS admitidos en la supervisión en tiempo de ejecución: GuardDuty lanzó inicialmente la supervisión en tiempo de ejecución para admitir únicamente los recursos de Amazon Elastic Kubernetes Service (Amazon EKS). Ahora, puede utilizar la característica de supervisión en tiempo de ejecución para disponer de detección de amenazas también para los recursos de AWS Fargate Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Compute Cloud (Amazon EC2).

GuardDuty no admite clústeres de Amazon EKS que se ejecuten en AWS Fargate.

En este documento y en otras secciones relacionadas con la supervisión en tiempo de ejecución, GuardDuty utiliza la terminología de tipo de recurso para referirse a los recursos de Amazon EKS, Fargate Amazon ECS y Amazon EC2.

La supervisión en tiempo de ejecución utiliza un agente de seguridad de GuardDuty que aporta visibilidad al comportamiento en tiempo de ejecución, como el acceso a archivos, la ejecución de procesos, los argumentos de línea de comandos y las conexiones de red. Para cada tipo de recurso que desee supervisar en busca de posibles amenazas, puede administrar el agente de seguridad correspondiente a ese tipo de recurso específico de forma automática o manual (a excepción de Fargate, solo Amazon ECS). Administrar el agente de seguridad automáticamente significa que permite a GuardDuty instalar y actualizar el agente de seguridad en su nombre. Por otra parte, al administrar manualmente el agente de seguridad para los recursos, usted será responsable de instalar y actualizar el agente de seguridad, según sea necesario.

Gracias a esta capacidad ampliada, GuardDuty puede ayudar a identificar amenazas potenciales que pueden tener como objetivo aplicaciones y datos que se ejecutan en las cargas de trabajo e instancias individuales, y responder ante estas. Por ejemplo, una amenaza puede empezar por comprometer un único contenedor que ejecuta una aplicación web vulnerable. Es posible que esta aplicación web tenga permisos de acceso a los contenedores y las cargas de trabajo subyacentes. En este escenario, las credenciales mal configuradas podrían dar lugar a un acceso más amplio a la cuenta y a los datos almacenados en ella.

Al analizar los eventos en tiempo de ejecución de los contenedores y cargas de trabajo individuales, GuardDuty puede identificar potencialmente si un contenedor y las credenciales de AWS asociadas

se han visto comprometidos en una fase inicial, y detectar intentos de escalar privilegios, solicitudes de API sospechosas y accesos maliciosos a los datos en el entorno.

Contenido

- [Funcionamiento](#)
- [¿Cómo funciona la prueba gratuita de 30 días en la supervisión en tiempo de ejecución?](#)
- [Requisitos previos para habilitar la Supervisión en tiempo de ejecución](#)
- [Habilitar la Supervisión en tiempo de ejecución de GuardDuty](#)
- [Administrar los agentes de seguridad de GuardDuty](#)
- [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#)
- [Configuración de la supervisión de la CPU y la memoria](#)
- [Uso de VPC compartida con Runtime Monitoring](#)
- [Utilizar la Infraestructura como Código \(IaC\) con agentes de seguridad automatizados de GuardDuty](#)
- [Tipos de eventos de tiempo de ejecución recopilados que utiliza GuardDuty](#)
- [Repositorio de Amazon ECR que aloja el agente de GuardDuty](#)
- [Dos agentes de seguridad en el mismo host subyacente](#)
- [Supervisión en tiempo de ejecución de EKS en GuardDuty](#)
- [Versiones del agente de seguridad de GuardDuty](#)
- [Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución](#)

Funcionamiento

Para utilizar la supervisión en tiempo de ejecución, debe habilitarla y luego administrar el agente de seguridad de GuardDuty. La siguiente lista explica este proceso en dos pasos:

1. Habilite la supervisión en tiempo de ejecución para la cuenta de manera que GuardDuty pueda aceptar los eventos en tiempo de ejecución que recibe de las instancias de Amazon EC2, los clústeres de Amazon ECS y las cargas de trabajo de Amazon EKS.
2. Administre el agente de GuardDuty para los recursos individuales cuyo comportamiento en tiempo de ejecución desee supervisar. Según el tipo de recurso, puede:

- Utilizar una configuración automática de agentes, en la que GuardDuty administra la implementación del agente y, automáticamente, un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC).
- Instalar el agente de manera manual, lo que requiere crear un punto de conexión de VPC como requisito previo.

El agente de seguridad utiliza el punto de conexión de VPC para enviar los eventos a GuardDuty, lo que garantiza que los datos permanezcan en la red de AWS. Este enfoque mejora la seguridad y permite a GuardDuty supervisar y analizar el comportamiento del tiempo de ejecución en todos sus recursos (Amazon EKS, Amazon EC2 y AWS Fargate-Amazon ECS). GuardDuty utiliza [roles de identidad de instancia](#) para autenticar el agente de seguridad para cada tipo de recurso y así enviar los eventos de tiempo de ejecución asociados al punto de conexión de VPC.

 Note

GuardDuty no le ofrece acceso a los eventos en tiempo de ejecución.

Al administrar el agente de seguridad (ya sea manualmente o a través de GuardDuty) en la supervisión en tiempo de ejecución de EKS o en la supervisión en tiempo de ejecución para instancias de EC2, y GuardDuty se encuentre actualmente implementado en una instancia de Amazon EC2 y recibe los [Tipos de eventos de tiempo de ejecución recopilados](#) de esta instancia, GuardDuty no cobrará a la Cuenta de AWS por el análisis de los registros de flujo de la VPC procedentes de esta instancia de Amazon EC2. Esto ayuda a GuardDuty a evitar el doble costo de uso en la cuenta.

En los siguientes temas se explica cómo funciona la habilitación de la supervisión en tiempo de ejecución y la administración del agente de seguridad de GuardDuty de forma diferente para cada tipo de recurso.

Contenido

- [Cómo funciona la supervisión en tiempo de ejecución con los clústeres de Amazon EKS](#)
- [Cómo funciona la supervisión en tiempo de ejecución con las instancias de Amazon EC2](#)
- [Cómo funciona la supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#)
- [Después de habilitar la supervisión en tiempo de ejecución](#)

Cómo funciona la supervisión en tiempo de ejecución con los clústeres de Amazon EKS

La supervisión en tiempo de ejecución utiliza un [complemento de EKS \(aws-guardduty-agent\)](#), también denominado agente de seguridad de GuardDuty. Después de que el agente de seguridad de GuardDuty se implementa en los clústeres de EKS, GuardDuty puede recibir eventos en tiempo de ejecución correspondientes a estos clústeres de EKS.

Notas

Runtime Monitoring admite los clústeres de Amazon EKS que se ejecutan en instancias de Amazon EC2 y en Amazon EKS Auto Mode.

Runtime Monitoring no admite los clústeres de Amazon EKS con los nodos híbridos de Amazon EKS ni los que se ejecutan en AWS Fargate.

Para obtener más información sobre estas características de Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

Puede supervisar los eventos en tiempo de ejecución de los clústeres de Amazon EKS a nivel de cuenta o de clúster. Puede administrar el agente de seguridad de GuardDuty solo para aquellos clústeres de Amazon EKS que desee supervisar para detectar amenazas. Puede administrar el agente de seguridad de GuardDuty ya sea manualmente o bien permitir que GuardDuty lo administre en su nombre, mediante la configuración automatizada del agente.

Cuando se utiliza el enfoque de configuración automatizada de agentes para permitir que GuardDuty administre la implementación del agente de seguridad en su nombre, se creará automáticamente un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC). El agente de seguridad entrega los eventos en tiempo de ejecución a GuardDuty. Para ello, utiliza este punto de conexión de Amazon VPC.

Junto con el punto de conexión de VPC, GuardDuty también crea un nuevo grupo de seguridad. Las reglas de entrada controlan el tráfico que puede llegar a los recursos asociados al grupo de seguridad. GuardDuty agrega reglas de entrada que coinciden con el rango CIDR de la VPC correspondiente al recurso, a la vez que se adapta cuando el rango de CIDR cambia. Para obtener más información, consulte [Rango de CIDR de la VPC](#) en la Guía del usuario de Amazon VPC.

Notas

- El uso del punto de conexión de VPC no conlleva ningún costo adicional.
- Utilizar una VPC centralizada con agente automatizado: cuando se utiliza la configuración de agente automatizado de GuardDuty para un tipo de recurso, GuardDuty creará un punto de conexión de VPC en su nombre para todas las VPC. Esto incluye la VPC centralizada y las VPC de radio. GuardDuty no admite la creación de un punto de conexión de VPC únicamente para la VPC centralizada. Para obtener más información sobre cómo funciona la VPC centralizada, consulte [Puntos de conexión de VPC de interfaz](#) en el documento técnico de AWS: Creación de una infraestructura de red de AWS de múltiples VPC escalable y segura.

Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS

Antes del 13 de septiembre de 2023, podía configurar GuardDuty para administrar el agente de seguridad en el nivel de cuenta. Este comportamiento indica que, de forma predeterminada, GuardDuty administrará el agente de seguridad en todos los clústeres de EKS que pertenezcan a una Cuenta de AWS. Ahora, GuardDuty ofrece una capacidad granular que lo ayuda a elegir los clústeres de EKS en los que quiere que GuardDuty administre el agente de seguridad.

Si decide [Administración manual del agente de seguridad de GuardDuty](#), puede seguir seleccionando los clústeres de EKS que desee supervisar. Sin embargo, para administrar el agente de forma manual, es un requisito previo crear un punto de conexión de VPC de Amazon para la Cuenta de AWS.

Note

Independientemente del enfoque que utilice para administrar el agente de seguridad de GuardDuty, la supervisión en tiempo de ejecución de EKS siempre está activada en el nivel de cuenta.

Temas

- [Administración del agente de seguridad a través de GuardDuty](#)

- [Administración manual del agente de seguridad de GuardDuty](#)

Administración del agente de seguridad a través de GuardDuty

GuardDuty implementa y administra el agente de seguridad en su nombre. En cualquier momento, puede supervisar los clústeres de EKS de su cuenta con uno de los siguientes enfoques.

Temas

- [Supervisar todos los clústeres de EKS](#)
- [Excluir determinados clústeres de EKS](#)
- [Incluir determinados clústeres de EKS](#)

Supervisar todos los clústeres de EKS

Utilice este enfoque cuando desee que GuardDuty implemente y administre el agente de seguridad para todos los clústeres de EKS en la cuenta. De forma predeterminada, GuardDuty también implementará el agente de seguridad en un clúster de EKS potencialmente nuevo creado en su cuenta.

Impacto de optar por este enfoque

- GuardDuty crea un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC) a través del cual el agente de seguridad de GuardDuty envía los eventos de tiempo de ejecución a GuardDuty. La creación del punto de conexión de VPC de Amazon al administrar el agente de seguridad a través de GuardDuty no conlleva ningún costo adicional.
- Es necesario que el nodo de trabajo tenga una ruta de red válida a un punto de conexión de VPC de guardduty-data activo. GuardDuty implementa el agente de seguridad en sus clústeres de EKS. Amazon Elastic Kubernetes Service (Amazon EKS) coordinará la implementación del agente de seguridad en los nodos de los clústeres de EKS.
- En función de la disponibilidad de las IP, GuardDuty selecciona la subred para crear un punto de conexión de VPC. Si utiliza topologías de red avanzadas, debe validar que la conectividad sea posible.

Excluir determinados clústeres de EKS

Utilice este enfoque cuando desee que GuardDuty administre el agente de seguridad correspondiente a todos los clústeres de EKS en la cuenta, pero excluya determinados clústeres de

EKS. Este método utiliza un enfoque basado en etiquetas¹ en el que puede etiquetar los clústeres de EKS para los que no desea recibir los eventos de tiempo de ejecución. La etiqueta predefinida debe tener `GuardDutyManaged=false` como par de clave-valor.

Impacto de optar por este enfoque

Este enfoque requiere que habilite la administración automática del agente de GuardDuty solo después de agregar etiquetas a los clústeres de EKS que desee excluir de la supervisión.

Por lo tanto, el impacto que se produce al [Administración del agente de seguridad a través de GuardDuty](#) también se aplica este enfoque. Al agregar etiquetas antes de habilitar la administración automática del agente de GuardDuty, GuardDuty no implementará ni administrará el agente de seguridad para los clústeres de EKS que estén excluidos de la supervisión.

Consideraciones

- Debe agregar el par clave-valor de la etiqueta como `GuardDutyManaged=false` para los clústeres de EKS determinados antes de habilitar la configuración automatizada del agente, de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS hasta que utilice la etiqueta.
- Debe impedir que se modifiquen las etiquetas, excepto por parte de identidades de confianza.

Important

Administre los permisos para modificar el valor de la etiqueta `GuardDutyManaged` de su clúster de EKS mediante políticas de control de servicios o políticas de IAM. Para obtener más información, consulte [Políticas de control de servicios \(SCP\)](#) en la Guía del usuario de AWS Organizations o [Control de acceso a los recursos de AWS mediante etiquetas](#) en la Guía del usuario de IAM.

- En el caso de un clúster de EKS potencialmente nuevo que no desee supervisar, asegúrese de agregar el par de clave-valor `GuardDutyManaged=false` al crear este clúster de EKS.
- Este enfoque también tendrá las mismas consideraciones que las especificadas para [Supervisar todos los clústeres de EKS](#).

Incluir determinados clústeres de EKS

Utilice este enfoque cuando desee que GuardDuty implemente y administre las actualizaciones del agente de seguridad únicamente para determinados clústeres de EKS en la cuenta. Este método

utiliza un enfoque basado en etiquetas¹ en el que puede etiquetar el clúster de EKS para el que desea recibir los eventos de tiempo de ejecución.

Impacto de optar por este enfoque

- Por medio del uso de etiquetas de inclusión, GuardDuty implementará y administrará automáticamente el agente de seguridad solamente para los clústeres de EKS determinados que hayan sido etiquetados con `GuardDutyManaged=true` como par de clave y valor.
- El uso de este enfoque también tendrá el mismo impacto que el especificado para [Supervisar todos los clústeres de EKS](#).

Consideraciones

- Si el valor de la etiqueta `GuardDutyManaged` no está establecido en `true`, la etiqueta de inclusión no funcionará como se esperaba y esto podría afectar a la supervisión del clúster de EKS.
- Para asegurarse de que se estén supervisando determinados clústeres de EKS, debe evitar que las etiquetas se modifiquen, salvo por parte de identidades de confianza.

Important

Administre los permisos para modificar el valor de la etiqueta `GuardDutyManaged` de su clúster de EKS mediante políticas de control de servicios o políticas de IAM. Para obtener más información, consulte [Políticas de control de servicios \(SCP\)](#) en la Guía del usuario de AWS Organizations o [Control de acceso a los recursos de AWS mediante etiquetas](#) en la Guía del usuario de IAM.

- En el caso de un clúster de EKS potencialmente nuevo que no desee supervisar, asegúrese de agregar el par de clave-valor `GuardDutyManaged=false` al crear este clúster de EKS.
- Este enfoque también tendrá las mismas consideraciones que las especificadas para [Supervisar todos los clústeres de EKS](#).

¹ Para obtener más información sobre el etiquetado de determinados clústeres de EKS, consulte [Etiquetado de los recursos de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Administración manual del agente de seguridad de GuardDuty

Utilice este enfoque cuando desee implementar y administrar manualmente el agente de seguridad de GuardDuty en todos los clústeres de EKS. Asegúrese de que la supervisión en tiempo de

ejecución de EKS esté habilitada en sus cuentas. Es posible que el agente de seguridad de GuardDuty no funcione según lo esperado si no habilita la supervisión en tiempo de ejecución de EKS.

Impacto de optar por este enfoque

Deberá coordinar la implementación del agente de seguridad de GuardDuty en los clústeres de EKS en las cuentas y Regiones de AWS en las que esta característica se encuentre disponible. Además, deberá actualizar la versión del agente cuando GuardDuty la publique. Para obtener más información sobre las versiones de los agentes para EKS, consulte [Versiones del agente de seguridad GuardDuty para los recursos de Amazon EKS](#).

Consideraciones

Debe admitir un flujo de datos seguro a la vez que supervisa y soluciona las deficiencias de cobertura a medida que se implementan continuamente nuevos clústeres y cargas de trabajo.

Cómo funciona la supervisión en tiempo de ejecución con las instancias de Amazon EC2

Las instancias de Amazon EC2 pueden ejecutar varios tipos de aplicaciones y cargas de trabajo en el entorno de AWS. Cuando se habilita la supervisión en tiempo de ejecución y se administra el agente de seguridad de GuardDuty, GuardDuty ayuda a detectar amenazas en las instancias de Amazon EC2 existentes y en las potencialmente nuevas. Además, esta característica es compatible con las instancias de Amazon EC2 administradas por Amazon ECS.

Note

Runtime Monitoring no admite aplicaciones que se ejecuten en [instancias administradas por Amazon ECS](#).

Al habilitar la supervisión en tiempo de ejecución, se consigue que GuardDuty esté preparado para consumir eventos en tiempo de ejecución tanto de procesos actualmente en ejecución como de procesos nuevos dentro de instancias de Amazon EC2. GuardDuty exige un agente de seguridad para enviar eventos en tiempo de ejecución desde la instancia de EC2 a GuardDuty.

En el caso de las instancias de Amazon EC2, el agente de seguridad de GuardDuty opera a nivel de instancia. Puede decidir si desea supervisar todas las instancias de Amazon EC2 en la cuenta o solo

algunas. Si desea administrar instancias determinadas, el agente de seguridad solo será necesario para estas instancias.

Además, GuardDuty puede consumir eventos en tiempo de ejecución de tareas nuevas y tareas existentes que se ejecuten en instancias de Amazon EC2 dentro de clústeres de Amazon ECS.

La supervisión en tiempo de ejecución ofrece las siguientes dos opciones para instalar el agente de seguridad de GuardDuty:

- [Utilice la configuración automatizada de agentes \(opción recomendada\)](#), or
- [Administrar el agente de seguridad manualmente](#)

Utilice la configuración automatizada de agentes a través de GuardDuty (opción recomendada)

Utilice la configuración automatizada del agente que permite a GuardDuty instalar el agente de seguridad en las instancias de Amazon EC2 en su nombre. GuardDuty también administra las actualizaciones del agente de seguridad.

De forma predeterminada, GuardDuty instala el agente de seguridad en todas las instancias de la cuenta. Si desea que GuardDuty instale y administre el agente de seguridad únicamente para determinadas instancias de EC2, agregue etiquetas de inclusión o exclusión a las instancias de EC2, según sea necesario.

En algunos casos, es posible que no desee supervisar los eventos en tiempo de ejecución de todas las instancias de Amazon EC2 pertenecientes a la cuenta. Para los casos en los que desee supervisar los eventos en tiempo de ejecución de una cantidad limitada de instancias, agregue una etiqueta de inclusión como `GuardDutyManaged:true` a estas instancias determinadas. Desde que está disponible la configuración automatizada de agentes para Amazon EC2, si la instancia de EC2 tiene una etiqueta de inclusión (`GuardDutyManaged:true`), GuardDuty respetará la etiqueta y administrará el agente de seguridad para las instancias seleccionadas incluso cuando no se habilite explícitamente la configuración automatizada de agentes.

Por otro lado, si existe una cantidad limitada de instancias de EC2 para las que no desea supervisar los eventos en tiempo de ejecución, agregue una etiqueta de exclusión (`GuardDutyManaged:false`) a estas instancias seleccionadas. GuardDuty respetará la etiqueta de exclusión y no instalará ni administrará el agente de seguridad para estos recursos de EC2.

Impact

Cuando se utiliza la configuración automatizada de agentes en una Cuenta de AWS u organización, se permite a GuardDuty realizar los siguientes pasos en su nombre:

- GuardDuty crea una asociación de SSM para todas las instancias de Amazon EC2 administradas por SSM y que aparecen en el Administrador de flotas en la consola <https://console.aws.amazon.com/systems-manager/>.
- Utilizar etiquetas de inclusión con la configuración automatizada del agente desactivada: después de habilitar la supervisión en tiempo de ejecución, si no habilita la configuración automatizada del agente pero agrega una etiqueta de inclusión a la instancia de Amazon EC2, significa que permite que GuardDuty administre el agente de seguridad en su nombre. La asociación de SSM instalará entonces el agente de seguridad en cada instancia que tenga la etiqueta de inclusión (`GuardDutyManaged:true`).
- Si habilita la configuración automatizada del agente: la asociación de SSM instalará entonces el agente de seguridad en todas las instancias de EC2 pertenecientes a la cuenta.
- Usar etiquetas de exclusión con la configuración automatizada de agentes: antes de habilitar la configuración automatizada de agentes, al agregar una etiqueta de exclusión a la instancia de Amazon EC2, se permite que GuardDuty evite la instalación y administración del agente de seguridad para la instancia seleccionada.

Ahora, al habilitar la configuración automatizada del agente, la asociación de SSM instalará y administrará el agente de seguridad en todas las instancias de EC2 excepto en aquellas etiquetadas con la etiqueta de exclusión.

- GuardDuty crea puntos de conexión de VPC en todas las VPC, incluidas las VPC compartidas, siempre que haya al menos una instancia de EC2 de Linux en esa VPC que no tenga el estado de instancia terminada o apagada. Esto incluye la VPC centralizada y las VPC de radio. GuardDuty no admite la creación de un punto de conexión de VPC únicamente para la VPC centralizada. Para obtener más información sobre cómo funciona la VPC centralizada, consulte [Puntos de conexión de VPC de interfaz](#) en el documento técnico de AWS: Creación de una infraestructura de red de AWS de múltiples VPC escalable y segura.

Para obtener información sobre los diferentes estados de las instancias, consulte [Ciclo de vida de las instancias](#) en la Guía del usuario de Amazon EC2.

GuardDuty también admite [Uso de VPC compartida con Runtime Monitoring](#). Cuando todos los requisitos previos son considerados para la organización y la Cuenta de AWS, GuardDuty utilizará la VPC compartida para recibir eventos en tiempo de ejecución.

 Note

El uso del punto de conexión de VPC no conlleva ningún costo adicional.

- Junto con el punto de conexión de la VPC, GuardDuty también crea un nuevo grupo de seguridad. Las reglas de entrada controlan el tráfico que puede llegar a los recursos asociados al grupo de seguridad. GuardDuty agrega reglas de entrada que coinciden con el rango CIDR de la VPC correspondiente al recurso, a la vez que se adapta cuando el rango de CIDR cambia. Para obtener más información, consulte [Rango de CIDR de la VPC](#) en la Guía del usuario de Amazon VPC.

Administrar el agente de seguridad manualmente

Existen dos formas de administrar manualmente el agente de seguridad para Amazon EC2:

- Utilice los documentos administrados de GuardDuty en AWS Systems Manager para instalar el agente de seguridad en las instancias de Amazon EC2 que ya son administradas por SSM.

Siempre que lance una nueva instancia de Amazon EC2, asegúrese de que esté habilitada para SSM.

- Utilice scripts del administrador de paquetes RPM (RPM) para instalar el agente de seguridad en las instancias de Amazon EC2, independientemente de si son administradas por SSM o no.

Siguiente paso

Para comenzar a utilizar la configuración de supervisión en tiempo de ejecución para supervisar las instancias de Amazon EC2, consulte [Requisitos previos para la compatibilidad con instancias de Amazon EC2](#).

Cómo funciona la supervisión en tiempo de ejecución con Fargate (solo Amazon ECS)

Cuando se habilita la supervisión en tiempo de ejecución, GuardDuty queda listo para consumir los eventos en tiempo de ejecución de una tarea. Estas tareas se ejecutan dentro de los clústeres de

Amazon ECS, que a su vez se ejecutan en las instancias de AWS Fargate. Para que GuardDuty reciba estos eventos en tiempo de ejecución, es necesario utilizar el agente de seguridad dedicado completamente administrado.

 Note

Runtime Monitoring no admite aplicaciones que se ejecuten en [instancias administradas por Amazon ECS](#).

Puede permitir que GuardDuty administre el agente de seguridad de GuardDuty en su nombre, mediante la configuración automatizada del agente para una cuenta o una organización de AWS. GuardDuty comenzará a implementar el agente de seguridad en las nuevas tareas de Fargate que se lancen en los clústeres de Amazon ECS. En la siguiente lista se especifica lo que se puede esperar al habilitar el agente de seguridad de GuardDuty.

Repercusiones de habilitar el agente de seguridad de GuardDuty

GuardDuty crea un punto de conexión de nube privada virtual (VPC) y un grupo de seguridad

- Cuando se implementa el agente de seguridad de GuardDuty, GuardDuty creará un punto de conexión de VPC a través del cual el agente de seguridad entrega los eventos en tiempo de ejecución a GuardDuty.

Junto con el punto de conexión de la VPC, GuardDuty también crea un nuevo grupo de seguridad. Las reglas de entrada controlan el tráfico que puede llegar a los recursos asociados al grupo de seguridad. GuardDuty agrega reglas de entrada que coinciden con el rango CIDR de la VPC correspondiente al recurso, a la vez que se adapta cuando el rango de CIDR cambia. Para obtener más información, consulte [Rango de CIDR de la VPC](#) en la Guía del usuario de Amazon VPC.

- Utilizar una VPC centralizada con agente automatizado: cuando se utiliza la configuración de agente automatizado de GuardDuty para un tipo de recurso, GuardDuty creará un punto de conexión de VPC en su nombre para todas las VPC. Esto incluye la VPC centralizada y las VPC de radio. GuardDuty no admite la creación de un punto de conexión de VPC únicamente para la VPC centralizada. Para obtener más información sobre cómo funciona la VPC centralizada, consulte [Puntos de conexión de VPC de interfaz](#) en el documento técnico de AWS: Creación de una infraestructura de red de AWS de múltiples VPC escalable y segura.
- El uso del punto de conexión de VPC no conlleva ningún costo adicional.

GuardDuty agrega un contenedor sidecar

En el caso de una nueva tarea o servicio de Fargate que se comienza a ejecutar, un contenedor de GuardDuty (sidecar) se asocia a cada contenedor dentro de la tarea de Amazon ECS Fargate. El agente de seguridad de GuardDuty se ejecuta dentro del contenedor de GuardDuty asociado. Esto ayuda a GuardDuty a recopilar los eventos en tiempo de ejecución de cada contenedor que se ejecuta dentro de estas tareas.

La imagen del contenedor sidecar de GuardDuty se almacena en Amazon Elastic Container Registry (Amazon ECR) y las capas de imágenes se almacenan en Amazon S3. Cuando comience la tarea, necesitará extraer esta imagen del ECR. Según la configuración de la red, esto puede requerir ajustes específicos para garantizar el acceso tanto al ECR como al S3. Por ejemplo, si se utilizan grupos de seguridad con acceso restringido, se tendrá que permitir el acceso a la lista de prefijos administrados de S3. Para obtener más información acerca de cómo hacerlo, consulte [Requisitos previos para el acceso a imágenes de contenedores](#).

Cuando se inicia una tarea de Fargate, si el contenedor de GuardDuty (sidecar) no se puede lanzar en buen estado, la supervisión en tiempo de ejecución por diseño no impedirá que se ejecuten las tareas.

Las tareas de Fargate son inmutables de forma predeterminada. GuardDuty no implementará el sidecar cuando una tarea ya se encuentre en estado de ejecución. Si desea supervisar un contenedor en una tarea que ya está en ejecución, puede detener la tarea e iniciarla de nuevo.

Enfoques al administrar el agente de seguridad de GuardDuty en los recursos de Amazon ECS-Fargate.

La supervisión en tiempo de ejecución brinda la opción de detectar posibles amenazas a la seguridad en todos los clústeres de Amazon ECS (nivel de cuenta) o en clústeres concretos (nivel de clúster) en la cuenta. Cuando se habilita la configuración automatizada del agente para cada tarea de Amazon ECS Fargate que se ejecutará, GuardDuty agregará un contenedor sidecar para cada carga de trabajo de contenedor dentro de esa tarea. El agente de seguridad de GuardDuty se implementa en este contenedor sidecar. De este modo, GuardDuty obtiene visibilidad del comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS.

La supervisión en tiempo de ejecución permite administrar el agente de seguridad de los clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Antes de configurar las cuentas, valore si desea supervisar el comportamiento en tiempo de ejecución de todos los contenedores que pertenecen a las tareas de Amazon ECS, o incluir o excluir recursos específicos. Tenga en cuenta los siguientes enfoques.

Supervisión de todos los clústeres de Amazon ECS

Este enfoque ayudará a detectar posibles amenazas a la seguridad a nivel de cuenta. Utilice este enfoque cuando desee que GuardDuty detecte posibles amenazas de seguridad para todos los clústeres de Amazon ECS pertenecientes a la cuenta.

Exclusión de clústeres de Amazon ECS específicos

Utilice este enfoque cuando desee que GuardDuty detecte posibles amenazas de seguridad para la mayoría de los clústeres de Amazon ECS del entorno de AWS, pero excluya algunos de los clústeres. Este enfoque ayuda a supervisar el comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS a nivel de clúster. Por ejemplo, la cantidad de clústeres de Amazon ECS que pertenecen a la cuenta es 1000. Sin embargo, solo desea supervisar 930 clústeres de Amazon ECS.

Este enfoque exige agregar una etiqueta de GuardDuty predefinida a los clústeres de Amazon ECS que no desea supervisar. Para obtener más información, consulte [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#).

Incluir clústeres de Amazon ECS específicos

Utilice este enfoque cuando desee que GuardDuty detecte posibles amenazas de seguridad para algunos de los clústeres de Amazon ECS. Este enfoque ayuda a supervisar el comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS a nivel de clúster. Por ejemplo, la cantidad de clústeres de Amazon ECS que pertenecen a la cuenta es 1000. Sin embargo, solo desea supervisar 230 clústeres.

Este enfoque exige agregar una etiqueta predefinida de GuardDuty a los clústeres de Amazon ECS que desea supervisar. Para obtener más información, consulte [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#).

Después de habilitar la supervisión en tiempo de ejecución

Después de habilitar la supervisión en tiempo de ejecución e instalar el agente de seguridad de GuardDuty en la cuenta independiente o en varias cuentas de miembro, podrá seguir los pasos que se indican a continuación para asegurarse de que la configuración del plan de protección funciona

según lo previsto, así como para supervisar la cantidad de memoria y CPU que utiliza el agente de seguridad de GuardDuty.

Evaluar la cobertura en tiempo de ejecución

GuardDuty recomienda que evalúe continuamente el estado de cobertura del recurso en el que ha implementado el agente de seguridad. La cobertura puede estar en buen estado o en mal estado. Cuando la cobertura está en buen estado, significa que GuardDuty recibe los eventos en tiempo de ejecución del recurso correspondiente cuando se produce una actividad a nivel del sistema operativo.

Cuando la cobertura pasa a estar en buen estado para el recurso, GuardDuty puede recibir los eventos en tiempo de ejecución y analizarlos para la detección de amenazas. Cuando GuardDuty detecta una amenaza potencial para la seguridad en las tareas o aplicaciones que se ejecutan en las instancias y cargas de trabajo de contenedores, GuardDuty genera [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#).

Además, puede configurar un Amazon EventBridge (EventBridge) para recibir una notificación cuando la cobertura pase de estar en mal estado a estar en buen estado, o viceversa. Para obtener más información, consulte [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Configurar la supervisión de CPU y memoria para el agente de seguridad de GuardDuty

Una vez que haya comprobado que la cobertura esté en buen estado, podrá evaluar el rendimiento del agente de seguridad para el tipo de recurso. En el caso de los clústeres de Amazon EKS que dispongan de la versión v1.5 o superior del agente de seguridad, GuardDuty permite configurar los parámetros del agente de seguridad (complemento). Para obtener más información, consulte [Configuración de la supervisión de la CPU y la memoria](#).

GuardDuty detecta posibles amenazas

A medida que GuardDuty comienza a recibir los eventos en tiempo de ejecución del recurso, comienza a analizarlos. Cuando GuardDuty detecta una posible amenaza para la seguridad en cualquiera de las instancias de Amazon EC2, los clústeres de Amazon ECS o los clústeres de Amazon EKS, genera uno o varios [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#). Puede acceder a los detalles del resultado para ver los detalles del recurso impactado.

¿Cómo funciona la prueba gratuita de 30 días en la supervisión en tiempo de ejecución?

El periodo de prueba gratuito de 30 días funciona de forma diferente para las nuevas cuentas de GuardDuty y las cuentas existentes que ya han habilitado la supervisión en tiempo de ejecución de EKS antes de que la capacidad de supervisión en tiempo de ejecución se ampliara a las instancias de Amazon EC2 y AWS Fargate (solo Amazon ECS).

Utilizo el periodo de prueba de GuardDuty o nunca he habilitado la supervisión en tiempo de ejecución de EKS

En la siguiente lista se explica cómo funciona el periodo de prueba gratuito de 30 días si ya utiliza el periodo de prueba de 30 días de GuardDuty o si nunca ha habilitado la supervisión en tiempo de ejecución de EKS:

- Cuando habilita GuardDuty por primera vez, las funciones de supervisión en tiempo de ejecución y supervisión en tiempo de ejecución de EKS no se habilitan de forma predeterminada.

Al habilitar la supervisión en tiempo de ejecución para la cuenta u organización, asegúrese de configurar también el agente de seguridad de GuardDuty para el recurso que desea supervisar para la detección de amenazas. Por ejemplo, si desea utilizar la supervisión en tiempo de ejecución para las instancias de Amazon EC2, después de habilitar la supervisión en tiempo de ejecución, también deberá configurar el agente de seguridad para Amazon EC2. Esto se puede hacer manualmente o automáticamente a través de GuardDuty.

- El plan de protección de supervisión en tiempo de ejecución se habilita a nivel de cuenta. El periodo de prueba gratuito de 30 días funciona a nivel del recurso. Después de que el agente de seguridad de GuardDuty se implementa en un tipo de recurso específico, la prueba gratuita de 30 días comenzará cuando GuardDuty reciba el primer evento en tiempo de ejecución asociado con este tipo de recurso. Por ejemplo, ha implementado el agente de GuardDuty a nivel de recurso (para una instancia de Amazon EC2, un clúster de Amazon ECS y un clúster de Amazon EKS). Cuando GuardDuty reciba el primer evento en tiempo de ejecución para una instancia de Amazon EC2, se iniciará la prueba gratuita de 30 días para Amazon EC2 solamente.
- Cuando se quiere habilitar únicamente la supervisión en tiempo de ejecución de EKS: al habilitar GuardDuty por primera vez, la supervisión en tiempo de ejecución de EKS no se habilita de forma predeterminada (después del lanzamiento de la supervisión en tiempo de ejecución). Deberá habilitar la supervisión en tiempo de ejecución de EKS. Para utilizarla óptimamente, asegúrese

de administrar el agente de seguridad de GuardDuty manualmente o habilite la configuración automatizada del agente de modo que GuardDuty lo administre en su nombre. El periodo de prueba gratuito de 30 días para la supervisión en tiempo de ejecución de EKS comienza cuando GuardDuty recibe el primer evento en tiempo de ejecución correspondiente al recurso de Amazon EKS.

Habilite la supervisión en tiempo de ejecución de EKS antes del lanzamiento de la supervisión en tiempo de ejecución

Utilice esta sección únicamente cuando la supervisión en tiempo de ejecución de EKS estaba habilitada para la Cuenta de AWS y ahora desea migrar a la supervisión en tiempo de ejecución.

En la siguiente lista se incluyen escenarios que se podrían aplicar a su caso de uso de la habilitación de la supervisión en tiempo de ejecución:

- En el caso de una cuenta GuardDuty existente con el plan de protección de Supervisión en tiempo de ejecución de EKS habilitado y que utiliza la experiencia de la Consola de GuardDuty para utilizar este plan de protección: con el anuncio de la Supervisión en tiempo de ejecución, la experiencia de la consola de Supervisión en tiempo de ejecución de EKS se ha consolidado en la Supervisión en tiempo de ejecución. La configuración existente para la Supervisión en tiempo de ejecución de EKS se mantiene sin cambios. Puede continuar el uso de la compatibilidad con la API y la CLI para realizar operaciones asociadas a la supervisión en tiempo de ejecución de EKS.
- Para utilizar la Supervisión en tiempo de ejecución de EKS como parte de la Supervisión en tiempo de ejecución, deberá configurar la Supervisión en tiempo de ejecución para la cuenta u organización. Para mantener la misma configuración para la Supervisión en tiempo de ejecución, consulte [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#). Sin embargo, esto no repercutirá en la prueba gratuita de 30 días del recurso de Amazon EKS.
- El plan de protección de Supervisión en tiempo de ejecución se habilita a nivel de cuenta por región. Una vez que el agente de seguridad de GuardDuty se implementa en uno de los tipos de recursos especificados (instancia de Amazon EC2 y clúster de Amazon ECS), la prueba gratuita de 30 días comenzará cuando GuardDuty reciba el primer evento en tiempo de ejecución relacionado con el recurso. Hay una prueba gratuita de 30 días relacionada con cada tipo de recurso.

Por ejemplo, después de habilitar la Supervisión en tiempo de ejecución, opta por implementar el agente de GuardDuty solo en una instancia de Amazon EC2, la prueba gratuita de 30 días de este recurso se iniciará solo cuando GuardDuty reciba el primer evento en tiempo de ejecución

correspondiente a una instancia de Amazon EC2. Más adelante, cuando implemente el agente de GuardDuty para Fargate (solo Amazon ECS), la prueba gratuita de 30 días de este recurso se iniciará solo cuando GuardDuty reciba el primer evento en tiempo de ejecución correspondiente al clúster de Amazon ECS. Puesto que ya la Supervisión en tiempo de ejecución de EKS está habilitada en la cuenta, GuardDuty no restablecerá la prueba gratuita de 30 días para un recurso de Amazon EKS.

Requisitos previos para habilitar la Supervisión en tiempo de ejecución

Para habilitar la supervisión en tiempo de ejecución y administrar el agente de seguridad de GuardDuty, debe cumplir los requisitos previos para cada tipo de recurso que desee supervisar para la detección de amenazas. Cada tipo de recurso tiene diferentes requisitos previos. Por ejemplo, GuardDuty admite diferentes distribuciones de SO en función del tipo de recurso.

Si solo desea supervisar los recursos de Amazon EC2, deberá seguir los requisitos previos para las instancias de Amazon EC2. Si posteriormente decide supervisar los recursos de Amazon EKS, deberá seguir los requisitos previos específicos de los clústeres de Amazon EKS.

En las siguientes secciones se indican los requisitos previos en función del tipo de recurso.

Contenido

- [Requisitos previos para la compatibilidad con instancias de Amazon EC2](#)
- [Requisitos previos para la compatibilidad con AWS Fargate \(solo con Amazon ECS\)](#)
- [Requisitos previos para la compatibilidad con clústeres de Amazon EKS](#)

Requisitos previos para la compatibilidad con instancias de Amazon EC2

En esta sección se incluyen los requisitos previos para supervisar el comportamiento en tiempo de ejecución de las instancias de Amazon EC2. Una vez cumplidos estos requisitos previos, consulte [Habilitar la Supervisión en tiempo de ejecución de GuardDuty](#).

Temas

- [Haga que SSM administre las instancias de EC2 \(solo para la configuración automatizada de agentes\)](#)
- [Validar los requisitos de arquitectura](#)

- [Validación de la política de control de servicios de la organización en un entorno de varias cuentas](#)
- [Al utilizar la configuración automatizada de agentes](#)
- [Límite de CPU y memoria para el agente de GuardDuty](#)
- [Siguiendo el siguiente paso](#)

Haga que SSM administre las instancias de EC2 (solo para la configuración automatizada de agentes)

GuardDuty usa AWS Systems Manager (SSM) para implementar, instalar y administrar de manera automática el agente de seguridad en sus instancias. Si planea instalar y administrar de manera manual el agente GuardDuty, no necesitará SSM.

Para administrar las instancias de Amazon EC2 con Systems Manager, consulte [Configurar Systems Manager para instancias de Amazon EC2](#) en la Guía del usuario de AWS Systems Manager.

Validar los requisitos de arquitectura

La arquitectura de la distribución del sistema operativo puede afectar el comportamiento del agente de seguridad de GuardDuty. Debe cumplir los siguientes requisitos antes de utilizar la Supervisión en tiempo de ejecución para instancias de Amazon EC2:

- La compatibilidad del kernel incluye eBPF, Tracepoints y Kprobe. Para las arquitecturas de CPU, Runtime Monitoring admite AMD64 (x64) y ARM64 (Graviton2 y versiones posteriores)¹.

En la siguiente tabla aparece la distribución del sistema operativo que se ha verificado que es compatible con el agente de seguridad de GuardDuty para las instancias de Amazon EC2.

Distribución del sistema operativo ²	Versión del kernel ³
Amazon Linux 2	5.4 ⁴ , 5.10 ⁴ , 5.15
Amazon Linux 2023	5.4 ⁴ , 5.10 ⁴ , 5.15, 6.1, 6.5, 6.8, 6.12
Ubuntu 20.04 y Ubuntu 22.04	5.4 ⁴ , 5.10 ⁴ , 5.15, 6.1, 6.5, 6.8
Debian 11 y Debian 12	5.4 ⁴ , 5.10 ⁴ , 5.15, 6.1, 6.5, 6.8

Distribución del sistema operativo ²	Versión del kernel ³
Ubuntu 24.04	6.8
	6.13 ⁵ , 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

1. Runtime Monitoring para recursos de Amazon EC2 no es compatible con la primera generación de instancias de Graviton, como los tipos de instancia A1.
2. Compatibilidad con varios sistemas operativos: GuardDuty ha verificado que Runtime Monitoring es compatible con la distribución operativa que figura en la tabla anterior. Si bien el agente de seguridad de GuardDuty puede funcionar en sistemas operativos que no figuran en la tabla anterior, el equipo de GuardDuty no puede garantizar el valor de seguridad esperado.
3. Para cualquier versión del kernel, debe establecer el marcador `CONFIG_DEBUG_INFO_BT` en `y` (que significa verdadero). Esto es necesario para que el agente de seguridad de GuardDuty pueda funcionar como se espera.
4. En las versiones 5.10 y anteriores del kernel, el agente de seguridad GuardDuty utiliza la memoria bloqueada en la RAM (`RLIMIT_MEMLOCK`) para funcionar según lo previsto. Si el valor `RLIMIT_MEMLOCK` del sistema es demasiado bajo, GuardDuty recomienda establecer los

límites duros y flexibles en al menos 32 MB. Para obtener información sobre cómo comprobar y modificar el valor `RLIMIT_MEMLOCK` predeterminado, consulte [Visualización y actualización de los valores `RLIMIT\_MEMLOCK`](#).

5.

Para Ubuntu 24.04, las versiones 6.13 y 6.14 del kernel solo admiten las versiones 1.9.0 y superiores del agente EC2.

- Requisitos adicionales: solo si dispone de Amazon ECS/Amazon EC2

En el caso de Amazon ECS/Amazon EC2, recomendamos que utilice las AMI optimizadas para Amazon ECS más recientes (con fecha del 29 de septiembre de 2023 o posterior), o que utilice la versión v1.77.0 del agente de Amazon ECS.

Visualización y actualización de los valores **`RLIMIT_MEMLOCK`**

Si el límite `RLIMIT_MEMLOCK` del sistema es demasiado bajo, es posible que el agente de seguridad GuardDuty no funcione según lo diseñado. GuardDuty recomienda que tanto los límites rígidos como los límites flexibles sean de 32 MB como mínimo. Si no actualiza los límites, GuardDuty no podrá supervisar los eventos de tiempo de ejecución de su recurso. Cuando `RLIMIT_MEMLOCK` supere los límites mínimos establecidos, la actualización de estos límites pasa a ser opcional.

Puede modificar el valor `RLIMIT_MEMLOCK` predeterminado antes o después de instalar el agente de seguridad GuardDuty.

Para ver los valores **`RLIMIT_MEMLOCK`**

1. Ejecuta `ps aux | grep guardduty`. Esto generará el ID del proceso (pid).
2. Copie el ID del proceso (pid) del resultado del comando anterior.
3. Ejecute `grep "Max locked memory" /proc/pid/limits` después de reemplazar el pid con el ID de proceso copiado del paso anterior.

Esto mostrará la cantidad máxima de memoria bloqueada para ejecutar el agente de seguridad GuardDuty.

Para actualizar los valores **`RLIMIT_MEMLOCK`**

1. Si el archivo `/etc/systemd/system.conf.d/NUMBER-limits.conf` existe, comente la línea `DefaultLimitMEMLOCK` de este archivo. Este archivo establece un valor predeterminado

RLIMIT_MEMLOCK con alta prioridad, que sobrescribe la configuración del archivo `/etc/systemd/system.conf`.

2. Abre el archivo `/etc/systemd/system.conf` y quita el comentario de la línea que contiene `#DefaultLimitMEMLOCK=`.
3. Actualice el valor predeterminado proporcionando límites RLIMIT_MEMLOCK fijos y flexibles de al menos 32 MB. La política actualizada debería ser así: `DefaultLimitMEMLOCK=32M:32M`. El formato es `soft-limit:hard-limit`.
4. Ejecuta `sudo reboot`.

Validación de la política de control de servicios de la organización en un entorno de varias cuentas

Si ha configurado una política de control de servicio (SCP) para administrar los permisos en la organización, valide que el límite de permisos permita la acción `guardduty:SendSecurityTelemetry`. Se necesita para que GuardDuty admita la Supervisión en tiempo de ejecución en diferentes tipos de recursos.

Si es una cuenta de miembro, contacte al administrador delegado asociado. Para obtener información sobre cómo administrar SCP para la organización, consulte [Políticas de control de servicios \(SCP\)](#).

Al utilizar la configuración automatizada de agentes

Para [Utilice la configuración automatizada de agentes \(opción recomendada\)](#), la Cuenta de AWS debe cumplir con los siguientes requisitos previos:

- Cuando se utilizan etiquetas de inclusión con configuración automatizada del agente, para que GuardDuty cree una asociación SSM para una nueva instancia, asegúrese de que la nueva instancia sea administrada por SSM y aparezca bajo el Administrador de flotas en la consola <https://console.aws.amazon.com/systems-manager/>.
- Al utilizar etiquetas de exclusión con configuración automatizada del agente
 - Agregue la etiqueta `GuardDutyManaged:false` antes de configurar el agente automatizado de GuardDuty para la cuenta.

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya habilitado la configuración automatizada del agente para Amazon

EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión estará cubierta por la configuración automatizada del agente de GuardDuty.

- Activa la opción Permitir etiquetas en los metadatos de las instancias. Esta configuración es necesaria porque GuardDuty necesita leer la etiqueta de exclusión del servicio de metadatos de instancias (IMDS) para determinar si debe excluir la instancia de la instalación del agente. Para obtener más información, consulte [Habilitar el acceso a etiquetas de instancia en los metadatos de la instancia](#) en la Guía del usuario de Amazon EC2.

Límite de CPU y memoria para el agente de GuardDuty

Límite de CPU

El límite máximo de CPU para el agente de seguridad GuardDuty asociado a instancias de Amazon EC2 es el 10 por ciento del total de núcleos vCPU. Por ejemplo, si la instancia de EC2 tiene 4 núcleos vCPU, el agente de seguridad puede utilizar un máximo del 40 por ciento del 400 por ciento total disponible.

Límite de memoria

De la memoria asociada a la instancia de Amazon EC2, existe una memoria limitada que el agente de seguridad de GuardDuty puede utilizar.

En la siguiente tabla aparece el límite de memoria.

Memoria de la instancia de Amazon EC2	Memoria máxima para el agente de GuardDuty
Menos de 8 GB	128 MB
Menos de 32 GB	256 MB
Mayor o igual que 32 GB	1 GB

Siguiente paso

El siguiente paso consiste en configurar la Supervisión en tiempo de ejecución y también administrar el agente de seguridad (automática o manualmente).

Requisitos previos para la compatibilidad con AWS Fargate (solo con Amazon ECS)

En esta sección se incluyen los requisitos previos para supervisar el comportamiento en tiempo de ejecución de los recursos de ECS de Fargate-Amazon. Una vez cumplidos estos requisitos previos, consulte [Habilitar la Supervisión en tiempo de ejecución de GuardDuty](#).

Temas

- [Validación de los requisitos de arquitectura](#)
- [Requisitos previos para el acceso a imágenes de contenedores](#)
- [Validación de la política de control de servicios de la organización en un entorno de varias cuentas](#)
- [Validación de permisos de roles y límites de permisos de políticas](#)
- [Límites de CPU y memoria](#)

Validación de los requisitos de arquitectura

La plataforma que utilice puede afectar a la forma en que el agente de seguridad de GuardDuty ayuda a GuardDuty a la hora de recibir los eventos en tiempo de ejecución de los clústeres de Amazon ECS. Debe validar que esté utilizando una de las plataformas verificadas.

Consideraciones iniciales:

La plataforma AWS Fargate para los clústeres de Amazon ECS debe ser Linux. La versión de plataforma correspondiente debe ser como mínimo 1.4.0, o LATEST. Para obtener más información sobre las versiones de plataforma, consulte [Versiones de plataforma Linux](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Aún no se admiten las versiones de la plataforma Windows.

Plataformas verificadas

La distribución del sistema operativo y la arquitectura de la CPU repercuten en la compatibilidad proporcionada por el agente de seguridad de GuardDuty. En la siguiente tabla aparece la configuración verificada para implementar el agente de seguridad de GuardDuty y configurar la Supervisión en tiempo de ejecución.

Distribución del sistema operativo ¹	Compatibilidad del kernel	Arquitectura de CPU x64 (AMD64)	Arquitectura de CPU Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Soportado	Compatible

¹Compatibilidad con varios sistemas operativos: GuardDuty ha verificado que Runtime Monitoring es compatible con los sistemas operativos que aparecen en la tabla anterior. Si bien el agente de seguridad de GuardDuty puede funcionar en sistemas operativos que no figuran en la tabla anterior, el equipo de GuardDuty no puede garantizar el valor de seguridad esperado.

Requisitos previos para el acceso a imágenes de contenedores

Los siguientes requisitos previos ayudan a acceder a la imagen del contenedor de sidecar de GuardDuty desde el repositorio de Amazon ECR.

Requisitos de los permisos

El rol de ejecución de tareas requiere determinados permisos de Amazon Elastic Container Registry (Amazon ECR) para descargar la imagen del contenedor del agente de seguridad de GuardDuty:

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

Para restringir aún más los permisos de Amazon ECR, puede agregar el URI del repositorio de Amazon ECR que aloja el agente de seguridad de GuardDuty para AWS Fargate (solo Amazon ECS). Para obtener más información, consulte [Repositorio de Amazon ECR que aloja el agente de GuardDuty](#).

Puede utilizar la política administrada [AmazonECSTaskExecutionRolePolicy](#) o agregar los permisos anteriores a la política de TaskExecutionRole.

Configuración de definición de tareas

Al crear o actualizar los servicios de Amazon ECS, debe proporcionar información de subred en la definición de la tarea:

La ejecución de las API [CreateService](#) y [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service requiere que se transmita la información de la subred. Para obtener más información, consulte las [definiciones de tareas de Amazon ECS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Requisitos de conectividad de red

Debe garantizar la conectividad de red para descargar la imagen del contenedor de GuardDuty desde Amazon ECR. Este requisito es específico de GuardDuty porque utiliza Amazon ECR para alojar su agente de seguridad. En función de la configuración de red, tendrá que implementar una de las siguientes opciones:

Opción 1: usar el acceso a la red pública (si está disponible)

Si sus tareas de Fargate se ejecutan en subredes con acceso a Internet saliente, no es necesaria ninguna configuración de red adicional.

Opción 2: Uso de puntos de conexión de Amazon VPC (para subredes privadas)

Si las tareas de Fargate se ejecutan en subredes privadas sin acceso a Internet, debe configurar puntos de conexión de VPC para ECR a fin de garantizar que se puede acceder a través de la red al URI del repositorio de ECR que aloja el agente de seguridad de GuardDuty. Sin estos puntos de conexión, las tareas de las subredes privadas no pueden descargar la imagen del contenedor de GuardDuty.

Para obtener instrucciones sobre la configuración del punto de conexión de VPC, consulte [Crear los puntos de conexión de VPC para Amazon ECR](#) en la Guía del usuario de Amazon Elastic Container Registry.

Para obtener información sobre cómo habilitar Fargate para descargar el contenedor de GuardDuty, consulte [Utilizar imágenes de Amazon ECR con Amazon ECS](#) en la Guía del usuario de Amazon Elastic Container Registry.

Configuración del grupo de seguridad

Las imágenes del contenedor GuardDuty están en Amazon ECR y requieren acceso a Amazon S3. Este requisito es específico para descargar imágenes de contenedores de Amazon ECR. En el caso de las tareas con acceso restringido a la red, debe configurar sus grupos de seguridad para permitir el acceso a S3.

Agregue una regla de salida a su grupo de seguridad que permita el tráfico a la [lista de prefijos administrados de S3 \(p1-xxxxxxx\) en el puerto 443](#). Para agregar una regla de salida, consulte [Configurar las reglas de un grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

Para ver las listas de prefijos administradas por AWS en la consola o describirlas mediante AWS Command Line Interface (AWS CLI), consulte las listas de [prefijos administradas por AWS](#) la Guía del usuario de Amazon VPC.

Validación de la política de control de servicios de la organización en un entorno de varias cuentas

En esta sección, se explica cómo validar la configuración de la política de control de servicios (SCP) para garantizar que Runtime Monitoring funcione según lo esperado en toda la organización.

Si ha configurado una o más políticas de control de servicio para administrar los permisos en la organización, debe validar que no niegue la acción `guardduty:SendSecurityTelemetry`. Para obtener información sobre cómo funcionan las SCP, consulte la [evaluación de los SCP](#) en la Guía del usuario de AWS Organizations.

Si es una cuenta de miembro, contacte al administrador delegado asociado. Para obtener información sobre cómo administrar las SCP para la organización, consulte [Políticas de control de servicios \(SCP\)](#) en la Guía del usuario de AWS Organizations.

Realice los siguientes pasos para todas las SCP que haya configurado en su entorno de cuentas múltiples:

La validación de **`guardduty:SendSecurityTelemetry`** no se deniega en SCP

1. Abra la consola de Organizations en <https://console.aws.amazon.com/organizations/>. Debe iniciar sesión como rol de IAM o iniciar sesión como usuario raíz ([no se recomienda](#)) en la cuenta de administración de la organización.
2. En el panel de navegación izquierdo, seleccione Políticas (Políticas). A continuación, en Tipos de políticas compatibles, seleccione Políticas de control de servicios.

3. En la página Políticas de control de servicios, elija el nombre de la política que desea adjuntar.
4. En la página de detalles de la política, consulte el contenido de esta política. Asegúrese de que no deniegue la acción `guardduty:SendSecurityTelemetry`.

La siguiente política de SCP es un ejemplo para no denegar la acción `guardduty:SendSecurityTelemetry`:

JSON

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

Si su política deniega esta acción, debe actualizarla. Para obtener más información, consulte [Actualización de una política de control de servicio \(SCP\)](#) en la Guía del usuario de AWS Organizations.

Validación de permisos de roles y límites de permisos de políticas

Siga los siguientes pasos para validar que los límites de permisos asociados al rol y a su política no impliquen la acción `guardduty:SendSecurityTelemetry` de restricción.

Para ver los límites de permisos de los roles y su política

1. Inicie sesión en la Consola de administración de AWS y abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, en Administración del acceso, elija Roles.
3. En la página Roles, seleccione el rol *TaskExecutionRole* que acaba de crear.

4. En la página del rol seleccionado, en la pestaña Permisos, amplía el nombre de la política asociada a este rol. A continuación, verifique que esta política no restrinja `guardduty:SendSecurityTelemetry`.
5. Si el límite de permisos está establecido, amplíe esta sección. A continuación, amplíe cada política para comprobar que no restrinja la acción `guardduty:SendSecurityTelemetry`. El aspecto de la respuesta debe ser parecido a [Example SCP policy](#).

Si es necesario, lleve a cabo una de las siguientes acciones:

- Para modificar la política, seleccione Editar. En la página Modificar los permisos de esta política, actualice la política en el editor de políticas. Asegúrese de que el esquema JSON siga siendo válido. A continuación, elija Siguiente. A continuación, puede revisar y guardar los cambios.
- Para cambiar este límite de permisos y elegir otro límite, elija Cambiar límite.
- Para eliminar este límite de permisos, seleccione Eliminar límite.

Para obtener más información sobre las políticas de IAM, consulte [Políticas y permisos en AWS Identity and Access Management](#) en la Guía del usuario de IAM.

Límites de CPU y memoria

En la definición de la tarea de Fargate, debe especificar el valor de CPU y memoria a nivel de tarea. En la siguiente tabla se indican las combinaciones válidas de valores de CPU y memoria a nivel de tarea, y el correspondiente límite máximo de memoria del agente de seguridad de GuardDuty para el contenedor de GuardDuty.

Valor de CPU	Valor de memoria	Límite máximo de memoria del agente de GuardDuty
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	

Valor de CPU	Valor de memoria	Límite máximo de memoria del agente de GuardDuty
2048 (2 vCPU)	Entre 4 GB y 16 GB en incrementos de 1 GB	
4096 (4 vCPU)	Entre 8 GB y 20 GB en incrementos de 1 GB	
8192 (8 vCPU)	Entre 16 GB y 28 GB en incrementos de 4 GB	256 MB
	Entre 32 GB y 60 GB en incrementos de 4 GB	512 MB
16384 (16 vCPU)	Entre 32 GB y 120 GB en incrementos de 8 GB	1 GB

Después de habilitar la Supervisión en tiempo de ejecución y evaluar que la cobertura del clúster esté en buen estado, podrá configurar y ver las métricas de Información de contenedores. Para obtener más información, [Configurar la supervisión en el clúster de Amazon ECS](#).

El siguiente paso consiste en configurar la Supervisión en tiempo de ejecución, así como el agente de seguridad.

Requisitos previos para la compatibilidad con clústeres de Amazon EKS

Esta sección incluye los requisitos previos para supervisar el comportamiento en tiempo de ejecución de los recursos de Amazon EKS. Estos requisitos previos son cruciales para que el agente GuardDuty funcione como se espera. Una vez cumplidos estos requisitos previos, consulte [Habilitar la Supervisión en tiempo de ejecución de GuardDuty](#) para empezar a monitorear los recursos.

Compatibilidad con características de Amazon EKS

Runtime Monitoring admite los clústeres de Amazon EKS que se ejecutan en instancias de Amazon EC2 y en Amazon EKS Auto Mode.

Runtime Monitoring no admite los clústeres de Amazon EKS con los nodos híbridos de Amazon EKS ni los que se ejecutan en AWS Fargate.

Para obtener más información sobre estas características de Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

Validación de los requisitos de arquitectura

La plataforma que utilice puede afectar a la forma en que el agente de seguridad de GuardDuty ayuda a GuardDuty a la hora de recibir los eventos de tiempo de ejecución de sus clústeres de EKS. Debe validar que esté utilizando una de las plataformas verificadas. Si administra el agente de GuardDuty manualmente, asegúrese de que la versión de Kubernetes sea compatible con la versión del agente de GuardDuty que está en uso actualmente.

Plataformas verificadas

La distribución del sistema operativo, la versión del kernel y la arquitectura de la CPU afectan a la compatibilidad que ofrece el agente de seguridad de GuardDuty. La compatibilidad del kernel incluye eBPF, Tracepoints y Kprobe. Para las arquitecturas de CPU, Runtime Monitoring es compatible con AMD64 (x64) y ARM64 (Graviton2 y versiones posteriores)¹.

En la siguiente tabla se muestra la configuración verificada para implementar el agente de seguridad de GuardDuty y configurar la supervisión en tiempo de ejecución de EKS.

Distribución del sistema operativo ²	Versión del kernel ³	Versión de Kubernetes compatible
Bottlerocket	5.4, 5.10, 5.15, 6.1 ⁴	v1.23 - v1.34
Ubuntu	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.34
Amazon Linux 2	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.34
Amazon Linux 2023 ⁵	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.34
RedHat 9.4	5.14 ⁴	v1.21 - v1.34
Fedora 34	5.11, 5.17	v1.21 - v1.34
Fedora 40	6.8	v1.28 - v1.34
Fedora 41	6.12	v1.28 - v1.34

Distribución del sistema operativo ²	Versión del kernel ³	Versión de Kubernetes compatible
CentOS Stream 9	5.14	v1.21 - v1.34

1. La Supervisión en tiempo de ejecución para clústeres de Amazon EKS no es compatible con la primera generación de instancias de Graviton, como los tipos de instancia A1.
2. Compatibilidad con varios sistemas operativos: GuardDuty ha verificado que Runtime Monitoring es compatible con la distribución operativa que figura en la tabla anterior. Si bien el agente de seguridad de GuardDuty puede funcionar en sistemas operativos que no figuran en la tabla anterior, el equipo de GuardDuty no puede garantizar el valor de seguridad esperado.
3. Para cualquier versión del kernel, debe establecer el marcador CONFIG_DEBUG_INFO_BTTF en y (que significa verdadero). Esto es necesario para que el agente de seguridad de GuardDuty pueda funcionar como se espera.
4. Actualmente, con la versión 6.1 del Kernel, GuardDuty no puede generar [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#) relacionados con [Eventos del sistema de nombres de dominio \(DNS\)](#).
5. La Supervisión en tiempo de ejecución admite AL2023 con el lanzamiento del agente de seguridad de GuardDuty v1.6.0 y superior. Para obtener más información, consulte [Versiones del agente de seguridad GuardDuty para los recursos de Amazon EKS](#).

Versiones de Kubernetes compatibles con el agente de seguridad de GuardDuty

En la siguiente tabla se muestran las versiones de Kubernetes para los clústeres de EKS compatibles con el agente de seguridad de GuardDuty.

Versión del agente de seguridad de GuardDuty del complemento de Amazon EKS	Versión de Kubernetes
v1.11.0 (más reciente: v1.11.0-eksbuild.2)	1.28 - 1.34
v1.10.0 (más reciente: v1.10.0-eksbuild.2)	1.21 - 1.33

Versión del agente de seguridad de GuardDuty del complemento de Amazon EKS	Versión de Kubernetes
v1.9.0 (más reciente: v1.9.0-eksbuild.2) v1.8.1 (más reciente: v1.8.1-eksbuild.2)	1.21 - 1.32
v1.7.1 v1.7.0 v1.6.1	1.21 - 1.31
Versión 1.6.0 v1.5.0 v1.4.1 v1.4.0 v1.3.1	1.21 - 1.29
v1.3.0 v1.2.0	1.21 - 1.28
v1.1.0	1.21 - 1.26
v1.0.0	1.21 - 1.25

Algunas de las versiones del agente de seguridad de GuardDuty llegarán al final del soporte estándar.

Para obtener información sobre las versiones de lanzamiento del agente, consulte [Versiones del agente de seguridad GuardDuty para los recursos de Amazon EKS](#).

Límites de CPU y memoria

En la siguiente tabla se muestran los límites de CPU y memoria del complemento de Amazon EKS para GuardDuty (aws-guardduty-agent).

Parámetro	Límite mínimo	Límite máximo
CPU	200m	1000m
Memoria	256 Mi	1024 Mi

Cuando utiliza el complemento Amazon EKS versión 1.5.0 o superior, GuardDuty brinda la capacidad de configurar el esquema del complemento para los valores de CPU y memoria. Para obtener información sobre el rango configurable, consulte [Parámetros y valores que se pueden configurar](#).

Después de habilitar la supervisión en tiempo de ejecución de EKS y evaluar el estado de la cobertura de sus clústeres de EKS, podrá configurar y ver las métricas de información de los contenedores. Para obtener más información, consulte [Configuración de la supervisión de la CPU y la memoria](#).

Validar la política de control de servicios de la organización

Si ha configurado una política de control de servicio (SCP) para administrar los permisos en la organización, valide que el límite de permisos no restrinja `guardduty:SendSecurityTelemetry`. Se necesita para que GuardDuty admita la Supervisión en tiempo de ejecución en diferentes tipos de recursos.

Si es una cuenta de miembro, contacte al administrador delegado asociado. Para obtener información sobre cómo administrar SCP para la organización, consulte [Políticas de control de servicios \(SCP\)](#).

Habilitar la Supervisión en tiempo de ejecución de GuardDuty

Antes de habilitar la Supervisión en tiempo de ejecución en la cuenta, asegúrese de que el tipo de recurso para el que desea supervisar los eventos en tiempo de ejecución sea compatible con los requisitos de la plataforma. Para obtener más información, consulte [Requisitos previos](#).

Si ha utilizado la Supervisión en tiempo de ejecución de EKS antes del lanzamiento de la Supervisión en tiempo de ejecución, puede utilizar las API para comprobar y actualizar la configuración existente para la Supervisión en tiempo de ejecución de EKS. También puede migrar la configuración existente de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución. Para obtener más información, consulte [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#).

 Note

Actualmente, en esta documentación se indican los pasos necesarios para habilitar la Supervisión en tiempo real para las cuentas y la organización únicamente mediante la consola. También puede habilitar la Supervisión en tiempo de ejecución mediante [Acciones de la API](#) o [AWS CLI para GuardDuty](#).

Puede configurar la Supervisión en tiempo de ejecución si sigue los pasos que se indican en los siguientes temas.

Contenido

- [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#)
- [Habilitar la Supervisión en tiempo de ejecución para una cuenta independiente](#)

Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas

En entornos de múltiples cuentas, solo la cuenta de administrador delegado de GuardDuty puede habilitar o desactivar la Supervisión en tiempo de ejecución para las cuentas de miembro, y administrar la configuración automatizada de agentes para los tipos de recursos pertenecientes a las cuentas de miembro en la organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro a través de AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

Para la cuenta de administrador delegado de GuardDuty

Para habilitar la Supervisión en tiempo de ejecución para la cuenta de administrador delegado de GuardDuty

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución.

4. Uso de Habilitar para todas las cuentas

Si desea habilitar la Supervisión en tiempo de ejecución para todas las cuentas que pertenecen a la organización, incluida la cuenta de administrador delegado de GuardDuty, seleccione **Habilitar para todas las cuentas**.

5. Uso de Configurar cuentas manualmente

Si desea habilitar la Supervisión en tiempo de ejecución para cada cuenta de miembro individualmente, elija **Configurar cuentas manualmente**.

- Seleccione **Habilitar** en la sección **Administrador delegado** (esta cuenta).

6. Para que GuardDuty reciba los eventos en tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS) utiliza las siguientes opciones para administrar el agente de seguridad para estos recursos:

Para habilitar el agente de seguridad de GuardDuty

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Para todas las cuentas de miembro

Para habilitar la Supervisión en tiempo de ejecución para todas las cuentas de miembro en la organización

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija **Supervisión en tiempo de ejecución**.
3. En la página **Supervisión en tiempo de ejecución**, en la pestaña **Configuración**, elija **Editar** en la sección **Configuración de la supervisión en tiempo de ejecución**.
4. Elija **Habilitar para todas las cuentas**.

5. Para que GuardDuty reciba los eventos en tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS) utiliza las siguientes opciones para administrar el agente de seguridad para estos recursos:

Para habilitar el agente de seguridad de GuardDuty

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Para todas las cuentas de miembro activas existentes

Para habilitar la Supervisión en tiempo de ejecución para las cuentas de miembro existentes en la organización

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con la cuenta de administrador delegado de GuardDuty para la organización.

2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la página Supervisión en tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración de la Supervisión en tiempo de ejecución.
4. En el panel Supervisión en tiempo de ejecución, en la sección Cuentas de miembro activas, seleccione Acciones.
5. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
6. Elija Confirmar.
7. Para que GuardDuty reciba los eventos en tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS) utiliza las siguientes opciones para administrar el agente de seguridad para estos recursos:

Para habilitar el agente de seguridad de GuardDuty

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)

- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

 Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Habilitar automáticamente la supervisión en tiempo de ejecución únicamente para las nuevas cuentas de miembro

Para habilitar la Supervisión en tiempo de ejecución para las nuevas cuentas de miembro en la organización

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con la cuenta de administrador delegado de GuardDuty de la organización.

2. En el panel de navegación, elija Supervisión en tiempo de ejecución
3. En la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución.
4. Elija Configurar cuentas manualmente.
5. Elija Habilitar automáticamente las cuentas de miembros nuevas.
6. Para que GuardDuty reciba los eventos en tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS) utiliza las siguientes opciones para administrar el agente de seguridad para estos recursos:

Para habilitar el agente de seguridad de GuardDuty

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)

- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Para determinadas cuentas de miembro activas únicamente

Para habilitar la Supervisión en tiempo de ejecución para cuentas de miembro activas individuales

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.
3. En la página Cuentas, revise los valores de las columnas Supervisión en tiempo de ejecución y Administrar agente automáticamente. Estos valores indican si la Supervisión en tiempo de ejecución y la administración del agente de GuardDuty están habilitadas o no habilitadas para la cuenta correspondiente.
4. En la tabla Cuentas, seleccione la cuenta para la que desea habilitar la Supervisión en tiempo de ejecución. Puede elegir varias cuentas a la vez.
5. Elija Confirmar.
6. Seleccione Editar planes de protección. Elija la acción apropiada.
7. Elija Confirmar.
8. Para que GuardDuty reciba los eventos en tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS) utiliza las siguientes opciones para administrar el agente de seguridad para estos recursos:

Para habilitar el agente de seguridad de GuardDuty

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Habilitar la Supervisión en tiempo de ejecución para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#).

Después de habilitar la Supervisión en tiempo de ejecución, asegúrese de instalar el agente de seguridad de GuardDuty mediante una configuración automática o una implementación manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Para habilitar la Supervisión en tiempo de ejecución en una cuenta independiente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, seleccione Habilitar para habilitar la Supervisión en tiempo de ejecución para la cuenta.
4. Para que GuardDuty reciba los eventos en tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS) utiliza las siguientes opciones para administrar el agente de seguridad para estos recursos:

Para habilitar el agente de seguridad de GuardDuty

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Administrar los agentes de seguridad de GuardDuty

Puede administrar el agente de seguridad de GuardDuty para el recurso que desea supervisar. Si desea supervisar más de un tipo de recurso, asegúrese de administrar el agente de GuardDuty para ese recurso.

Los siguientes temas resultan útiles para los pasos a seguir para administrar el agente de seguridad.

Contenido

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)
- [Configurar los parámetros del agente de seguridad de GuardDuty \(complemento\) para Amazon EKS](#)
- [Validar la configuración del punto de conexión de VPC](#)

Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2

Esta sección incluye los pasos para habilitar el agente automatizado de GuardDuty para los recursos de Amazon EC2 en la cuenta independiente o en un entorno de varias cuentas.

Antes de continuar, asegúrese de cumplir todos los [Requisitos previos para la compatibilidad con instancias de Amazon EC2](#).

Si va a pasar de administrar el agente de GuardDuty manualmente a habilitar el agente automatizado de GuardDuty, antes de seguir los pasos para habilitar el agente automatizado de GuardDuty, consulte [Pasar del agente manual de Amazon EC2 al agente automatizado](#).

Habilitar el agente de GuardDuty para los recursos de Amazon EC2 en un entorno de varias cuentas

En entornos con varias cuentas, solo la cuenta de administrador delegado de GuardDuty puede habilitar o desactivar la configuración automática del agente para los tipos de recursos

pertenecientes a las cuentas de miembro en la organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro a través de AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

Para la cuenta de administrador delegado de GuardDuty

Configure for all instances

Si eligió Habilitar para todas las cuentas para la Supervisión en tiempo de ejecución, elija una de las siguientes opciones para la cuenta de administrador delegado de GuardDuty:

- Opción 1

En Configuración automatizada del agente, en la sección EC2, seleccione Habilitar para todas las cuentas.

- Opción 2

- En Configuración automatizada del agente, en la sección EC2, seleccione Configurar cuentas manualmente.

- En Administrador delegado (esta cuenta), elija Habilitar.

- Seleccione Save.

Si elige Configurar cuentas manualmente en la sección Supervisión en tiempo de ejecución, haga lo siguiente:

- En Configuración automatizada del agente, en la sección EC2, seleccione Configurar cuentas manualmente.

- En Administrador delegado (esta cuenta), elija Habilitar.

- Seleccione Save.

Independientemente de la opción que elija para habilitar la configuración automatizada del agente para la cuenta de administrador delegado de GuardDuty, puede comprobar que la asociación de SSM que GuardDuty crea instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a esta cuenta.

1. Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.

2. Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete). Observe que la clave de etiqueta aparece como Instancelds.

Using inclusion tag in selected instances

Para configurar el agente de GuardDuty para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta GuardDutyManaged:true a las instancias que desee que GuardDuty supervise y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Al agregar esta etiqueta, permitirá a GuardDuty instalar y administrar el agente de seguridad para estas instancias de EC2 seleccionadas. No es necesario habilitar la configuración automática del agente de forma explícita.

3. Puede verificar que la asociación de SSM que GuardDuty crea instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.

- Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete) que se crea. La clave de etiqueta aparece como tag:GuardDutyManaged.

Using exclusion tag in selected instances

Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya habilitado la configuración automatizada del agente para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión estará cubierta por la configuración automatizada del agente de GuardDuty.

Para configurar el agente de GuardDuty para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta `GuardDutyManaged:false` a las instancias que no desee que GuardDuty supervise ni detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para que las [etiquetas de exclusión estén disponibles](#) en los metadatos de la instancia, siga los siguientes pasos:
 - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
 - b. En el menú Acciones, elija Configuración de la instancia.
 - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Habilitar automáticamente para todas las cuentas de miembro

 Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Configure for all instances

En los siguientes pasos, se supone que seleccionó Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución:

1. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente para Amazon EC2.

2. Puedes verificar que la asociación de SSM que GuardDuty crea (GuardDutyRuntimeMonitoring-do-not-delete) instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenecen a esta cuenta.
 - a. Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.
 - b. Abra la pestaña Destinos correspondiente a la asociación de SSM. Observe que la clave de etiqueta aparece como Instancelds.

Using inclusion tag in selected instances

Para configurar el agente de GuardDuty para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta GuardDutyManaged:true a las instancias de EC2 que desee que GuardDuty supervise y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Al agregar esta etiqueta, permitirá a GuardDuty instalar y administrar el agente de seguridad para estas instancias de EC2 seleccionadas. No es necesario habilitar la configuración automática del agente de forma explícita.

3. Puede verificar que la asociación de SSM que GuardDuty crea instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a la cuenta.
 - a. Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.
 - b. Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete). Observe que la clave de etiqueta aparece como Instancelds.

Using exclusion tag in selected instances

Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya habilitado la configuración automatizada del agente para

Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión estará cubierta por la configuración automatizada del agente de GuardDuty.

Para configurar el agente de seguridad de GuardDuty para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta `GuardDutyManaged:false` a las instancias que no desee que GuardDuty supervise ni detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para que las [etiquetas de exclusión estén disponibles](#) en los metadatos de la instancia, siga los siguientes pasos:
 - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
 - b. En el menú Acciones, elija Configuración de la instancia.
 - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Habilitar automáticamente solo para nuevas cuentas de miembro

La cuenta de administrador delegado de GuardDuty puede establecer la configuración automatizada del agente para que el recurso de Amazon EC2 se habilite automáticamente para las nuevas cuentas de miembro a medida que se unen a la organización.

Configure for all instances

En los siguientes pasos se presupone que ha seleccionado Habilitar automáticamente para nuevas cuentas de miembro en la sección Supervisión en tiempo de ejecución:

1. En el panel de navegación, elija Supervisión en tiempo de ejecución.
2. En la página Supervisión en tiempo de ejecución, elija Editar.
3. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que siempre que una nueva cuenta se una a la organización, la configuración automatizada del agente para Amazon EC2 se habilitará automáticamente para la cuenta. Únicamente la cuenta de administrador delegado de GuardDuty de la organización puede modificar esta selección.
4. Seleccione Save.

Cuando una nueva cuenta de miembro se une a la organización, esta configuración se habilitará para esta automáticamente. Para que GuardDuty administre el agente de seguridad para las instancias de Amazon EC2 que pertenecen a esta nueva cuenta de miembro, asegúrese de que se cumplen todos los requisitos previos [Para la instancia de EC2](#).

Cuando se crea una asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete), puede comprobar que la asociación de SSM instalará y administrará el agente de seguridad en todas las instancias de EC2 pertenecientes a la nueva cuenta de miembro.

- Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.
- Abra la pestaña Destinos correspondiente a la asociación de SSM. Observe que la clave de etiqueta aparece como Instancelds.

Using inclusion tag in selected instances

Para configurar el agente de seguridad de GuardDuty para determinadas instancias seleccionadas en la cuenta

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta GuardDutyManaged:true a las instancias que desee que GuardDuty supervise y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Al agregar esta etiqueta permitirá a GuardDuty instalar y administrar el agente de seguridad para estas instancias seleccionadas. No es necesario habilitar explícitamente la configuración automática del agente.

3. Puede verificar que la asociación de SSM que GuardDuty crea instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.
 - a. Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.
 - b. Abra la pestaña Destinos correspondiente a la asociación de SSM que se crea. La clave de etiqueta aparece como tag:GuardDutyManaged.

Using exclusion tag in selected instances

Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya habilitado la configuración automatizada del agente para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión estará cubierta por la configuración automatizada del agente de GuardDuty.

Para configurar el agente de seguridad de GuardDuty para instancias específicas en la cuenta independiente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta GuardDutyManaged:false a las instancias que no desee que GuardDuty supervise ni detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para que las [etiquetas de exclusión estén disponibles](#) en los metadatos de la instancia, siga los siguientes pasos:
 - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
 - b. En el menú Acciones, elija Configuración de la instancia.
 - c. Elija Permitir etiquetas en los metadatos de la instancia.

4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Solo determinadas cuentas de miembro seleccionadas

Configure for all instances

1. En la página Cuentas, seleccione una o varias cuentas para las que desee habilitar la Configuración automatizada del agente de Supervisión en tiempo de ejecución (Amazon EC2). Asegúrese de que las cuentas que seleccione en este paso ya tienen habilitada la Supervisión en tiempo de ejecución.
2. En Editar planes de protección, elija la opción adecuada para habilitar la Configuración automatizada del agente de Supervisión en tiempo de ejecución (Amazon EC2).
3. Elija Confirmar.

Using inclusion tag in selected instances

Para configurar el agente de seguridad de GuardDuty para instancias seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta GuardDutyManaged:true a las instancias que desee que GuardDuty supervise y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Al agregar esta etiqueta permitirá a GuardDuty administrar el agente de seguridad para las instancias de Amazon EC2 etiquetadas. No necesita habilitar explícitamente la configuración automatizada del agente (Supervisión en tiempo de ejecución: configuración automatizada del agente (EC2)).

Using exclusion tag in selected instances

Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya habilitado la configuración automatizada del agente para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión estará cubierta por la configuración automatizada del agente de GuardDuty.

Para configurar el agente de seguridad de GuardDuty para instancias seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta `GuardDutyManaged:false` a las instancias EC2 para las que no desee que GuardDuty supervise ni detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para que las [etiquetas de exclusión estén disponibles](#) en los metadatos de la instancia, siga los siguientes pasos:
 - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
 - b. En el menú Acciones, elija Configuración de la instancia.
 - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Habilitar el agente automatizado de GuardDuty para los recursos de Amazon EC2 en una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#).

Después de habilitar la Supervisión en tiempo de ejecución, asegúrese de instalar el agente de seguridad de GuardDuty mediante una configuración automática o una implementación manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Según su preferencia de supervisar todos o algunos recursos de Amazon EC2, elija el método que prefiera y siga los pasos que se indican en la tabla siguiente.

Configure for all instances

Para configurar la Supervisión en tiempo de ejecución para todas las instancias en la cuenta independiente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, elija Editar.
4. En la sección EC2, elija Habilitar.
5. Seleccione Save.
6. Puede verificar que la asociación de SSM que GuardDuty crea instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a la cuenta.
 - a. Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.
 - b. Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete). Observe que la clave de etiqueta aparece como Instancelds.

Using inclusion tag in selected instances

Para configurar el agente de seguridad de GuardDuty para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Agregue la etiqueta `GuardDutyManaged:true` a las instancias que desee que GuardDuty supervise y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Puede verificar que la asociación de SSM que GuardDuty crea instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.

- Abra la pestaña Destinos correspondiente a la asociación de SSM (`GuardDutyRuntimeMonitoring-do-not-delete`) que se crea. La clave de etiqueta aparece como `tag:GuardDutyManaged`.

Using exclusion tag in selected instances

Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya habilitado la configuración automatizada del agente para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión estará cubierta por la configuración automatizada del agente de GuardDuty.

Para configurar el agente de seguridad de GuardDuty para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.

2. Agregue la etiqueta `GuardDutyManaged:false` a las instancias que no desee que GuardDuty supervise ni detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para que las [etiquetas de exclusión estén disponibles](#) en los metadatos de la instancia, siga los siguientes pasos:
 - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
 - b. Seleccione la instancia para la que desea permitir etiquetas.
 - c. En el menú Acciones, elija Configuración de la instancia.
 - d. Elija Permitir etiquetas en los metadatos de la instancia.
 - e. En Acceso a etiquetas en metadatos de instancia, seleccione Permitir.
 - f. Seleccione Save.
4. Después de agregar la etiqueta de exclusión, siga los mismos pasos que se indican en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Pasar del agente manual de Amazon EC2 al agente automatizado

Esta sección se aplica a la Cuenta de AWS si antes administraba el agente de seguridad manualmente y ahora desea utilizar la configuración automatizada del agente de GuardDuty. Si esto no se aplica a su caso, continúe con la configuración del agente de seguridad para la cuenta.

Cuando habilita el agente automatizado de GuardDuty, GuardDuty administra el agente de seguridad en su nombre. Para obtener información sobre los pasos que GuardDuty sigue, consulte [Utilice la configuración automatizada de agentes \(opción recomendada\)](#).

Eliminar recursos

Eliminar asociación de SSM

- Elimine cualquier asociación de SSM que pueda haber creado al administrar manualmente el agente de seguridad para Amazon EC2. Para obtener más información, consulte [Eliminar una asociación](#).
- Esto se hace de manera que GuardDuty pueda hacerse cargo de la administración de acciones de SSM ya sea que se usen agentes automatizados a nivel de cuenta o a nivel de instancia (mediante el uso de etiquetas de inclusión o exclusión). Para obtener más información sobre qué acciones de SSM puede realizar GuardDuty, consulte [Permisos de roles vinculados a servicios de GuardDuty](#).
- Cuando se elimina una asociación de SSM que fue creada previamente para administrar el agente de seguridad manualmente, es posible que transcurra un breve periodo de tiempo durante el cual GuardDuty crea una asociación de SSM para administrar el agente de seguridad automáticamente. Es posible que durante este periodo se produzcan conflictos relacionados con la programación de SSM. Para obtener más información, consulte [Programación de SSM en Amazon EC2](#).

Administre las etiquetas de inclusión y exclusión para las instancias de Amazon EC

- Etiquetas de inclusión: cuando no habilita la configuración automática del agente de GuardDuty, pero etiqueta alguna de las instancias de Amazon EC2 con una etiqueta de inclusión (`GuardDutyManaged:true`), GuardDuty crea una asociación de SSM que instalará y administrará el agente de seguridad en las instancias de EC2 seleccionadas. Este es un comportamiento esperado que ayuda a administrar el agente de seguridad únicamente en instancias de EC2 seleccionadas. Para obtener más información, consulte [Cómo funciona la supervisión en tiempo de ejecución con las instancias de Amazon EC2](#).

Para evitar que GuardDuty instale y administre el agente de seguridad, elimine la etiqueta de inclusión de estas instancias de EC2. Para obtener más información, consulte [Agregar y eliminar etiquetas](#) en la Guía del usuario de Amazon EC2.

- Etiquetas de exclusión: si desea habilitar la configuración automática del agente de GuardDuty para todas las instancias de EC2 en la cuenta, asegúrese de que ninguna instancia de EC2 esté etiquetada con una etiqueta de exclusión (`GuardDutyManaged:false`).

Administrar manualmente el agente de seguridad para el recurso de Amazon EC2

En esta sección se indican los pasos a seguir para instalar y actualizar manualmente el agente de seguridad para los recursos de Amazon EC2.

Después de habilitar la Supervisión en tiempo de ejecución, necesitará instalar el agente de seguridad GuardDuty manualmente. Para administrar el agente de seguridad de GuardDuty manualmente, primero debe crear un punto de conexión de Amazon VPC manualmente. Después de esto, puede instalar el agente de seguridad de modo que GuardDuty comience a recibir los eventos en tiempo de ejecución de las instancias de Amazon EC2. Cuando GuardDuty lanza una nueva versión de agente para este recurso, se puede actualizar la versión del agente en la cuenta.

En los siguientes temas se incluyen los pasos a seguir para administrar de forma continua el agente de seguridad para los recursos de Amazon EC2.

Temas

- [Requisito previo: crear manualmente el punto de conexión de Amazon VPC](#)
- [Instalación manual del agente de seguridad](#)
- [Actualizar manualmente el agente de seguridad de GuardDuty para una instancia de Amazon EC2](#)

Requisito previo: crear manualmente el punto de conexión de Amazon VPC

Antes de poder instalar el agente de seguridad GuardDuty, debe crear un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC). Esto ayudará a GuardDuty a recibir los eventos en tiempo de ejecución de las instancias de Amazon EC2.

Note

El uso del punto de conexión de VPC no conlleva ningún costo adicional.

Para crear un punto de conexión de Amazon VPC

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, en Nube privada VPC, seleccione Puntos de conexión.

3. Seleccione Crear punto de conexión.
4. En la página Crear punto de conexión, en Categoría de servicio, elija Otros servicios de punto de conexión.
5. En Nombre del servicio, escriba **com.amazonaws.us-east-1.guardduty-data**.

Asegúrese de sustituir **us-east-1** por la Región de AWS. Debe ser la misma región que la instancia de Amazon EC2 que pertenece al ID de la cuenta de AWS.

6. Elija Verificar el servicio.
7. Una vez que el nombre del servicio se haya verificado correctamente, elija la VPC en la que reside la instancia. Agregue la siguiente política para restringir el uso de puntos de conexión de Amazon VPC únicamente a la cuenta especificada. Con el valor de Condition de la organización que se indica debajo de esta política, puede actualizar la siguiente política para restringir el acceso a su punto de conexión. Para proporcionar compatibilidad con el punto de conexión de Amazon VPC a ID de cuenta específicos de la organización, consulte [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": ""
    }
  ]
}
```

```
}
```

El ID de cuenta de `aws:PrincipalAccount` debe coincidir con la cuenta que contiene la VPC y el punto de conexión de VPC. En la siguiente lista se indica cómo compartir el punto de conexión de VPC con otros ID de cuenta de AWS:

- Para especificar varias cuentas para acceder al punto de conexión de VPC, sustituya `"aws:PrincipalAccount: "111122223333"` por el siguiente bloque:

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

Asegúrese de sustituir los ID de cuenta de AWS por los ID de las cuentas que deben acceder al punto de conexión de VPC.

- Para permitir que todos los miembros de una organización accedan al punto de conexión de VPC, sustituya `"aws:PrincipalAccount: "111122223333"` por la siguiente línea:

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

Asegúrese de sustituir la organización `o-abcdef0123` por el ID de la organización.

- Para restringir el acceso a un recurso mediante un ID de organización, agregue el `ResourceOrgID` a la política. Para obtener más información, consulte [aws:ResourceOrgID](#) en la Guía del usuario de IAM.

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

8. En Configuración adicional, seleccione Habilitar nombre de DNS.
9. En Subredes, elija las subredes en las que reside la instancia.
10. En Grupos de seguridad, elija un grupo de seguridad que tenga habilitado el puerto de entrada 443 desde la VPC (o la instancia de Amazon EC2). Si aún no dispone de un grupo de seguridad que tenga habilitado un puerto de entrada 443, consulte [Crear un grupo de seguridad para la VPC](#) en la Guía del usuario de Amazon VPC.

Si se produce un problema al restringir los permisos de entrada a la VPC (o instancia), puede utilizar el puerto de entrada 443 desde cualquier dirección IP (`0.0.0.0/0`). Sin

embargo, GuardDuty recomienda utilizar direcciones IP que coincidan con el bloque de CIDR correspondiente a la VPC. Para obtener más información, consulte [Bloques de CIDR de VPC](#) en la Guía del usuario de Amazon VPC.

Una vez que haya seguido los pasos, consulte [Validar la configuración del punto de conexión de VPC](#) para asegurarse de que el punto de conexión de VPC se configuró correctamente.

Instalación manual del agente de seguridad

GuardDuty ofrece los dos siguientes métodos para instalar el agente de seguridad de GuardDuty en las instancias de Amazon EC2. Antes de continuar, asegúrese de seguir los pasos que se indican en [Requisito previo: crear manualmente el punto de conexión de Amazon VPC](#).

Elija el método de acceso que prefiera para instalar el agente de seguridad en los recursos de Amazon EC2.

- [Método 1: usar AWS Systems Manager](#): este método requiere que AWS Systems Manager administre la instancia de Amazon EC2.
- [Método 2: utilizar administradores de paquetes de Linux](#): puede utilizar este método independientemente de que AWS Systems Manager administre las instancias de Amazon EC2 o no. Según las [distribuciones de sistema operativo](#), puede elegir un método adecuado para instalar scripts RPM o Debian. Si usa la plataforma Fedora, debe usar este método para instalar el agente.

Método 1: usar AWS Systems Manager

Para utilizar este método, asegúrese de que AWS Systems Manager administre las instancias de Amazon EC2 y, a continuación, instale el agente.

Instancia de Amazon EC2 administrada por AWS Systems Manager

Siga los pasos que se indican a continuación para que AWS Systems Manager administre las instancias de Amazon EC2.

- [AWS Systems Manager](#) ayuda a administrar las aplicaciones y recursos de AWS de forma integral, así como a hacer posibles operaciones seguras a escala.

Para administrar las instancias de Amazon EC2 con AWS Systems Manager, consulte [Configurar Systems Manager para instancias de Amazon EC2](#) en la Guía del usuario de AWS Systems Manager.

- En la siguiente tabla aparecen los nuevos documentos de AWS Systems Manager administrados por GuardDuty:

Nombre del documento	Tipo de documento	Finalidad
AmazonGuardDuty-RunTimeMonitoringSsmPlugin	Distributor	Para empaquetar el agente de seguridad de GuardDuty.
AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin	Comando	Para ejecutar el script de instalación/desinstalación para instalar el agente de seguridad GuardDuty.

Para obtener más información sobre AWS Systems Manager, consulte [Documentos de Systems Manager de Amazon EC2](#) en la Guía del usuario de AWS Systems Manager.

Para servidores de Debian

Las imágenes de máquina de Amazon (AMI) para el servidor de Debian proporcionadas por AWS requieren que instale el agente de AWS Systems Manager (agente SSM). Deberá seguir un paso adicional para instalar el agente de SSM y hacer que SSM administre las instancias de servidor de Debian de Amazon EC2. Para obtener información sobre los pasos que debe seguir, consulte [Instalación manual del agente de SSM en instancias de servidor Debian](#) en la Guía del usuario de AWS Systems Manager.

Para instalar el agente de GuardDuty para una instancia de Amazon EC2 mediante AWS Systems Manager

- Abra la consola de AWS Systems Manager en <https://console.aws.amazon.com/systems-manager/>.
- En el panel de navegación, elija Documentos
- En Propiedad de Amazon, elija AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.

4. Elija Run Command (Ejecutar comando).
5. Ingrese los siguientes parámetros del Comando de ejecución
 - Acción: elija Instalar.
 - Tipo de instalación: elija Instalar o desinstalar.
 - Nombre: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
 - Versión: si se deja vacío, obtendrá la versión más reciente del agente de seguridad de GuardDuty. Para obtener más información acerca de las versiones de lanzamiento, [Versiones del agente de seguridad de GuardDuty para instancias de Amazon EC2](#).
6. Seleccione la instancia de Amazon EC2 de destino. Puede seleccionar una o más instancias de Amazon EC2. Para obtener más información, consulte [Ejecución de comandos de AWS Systems Manager desde la consola](#) en la Guía de usuario de AWS Systems Manager
7. Valide si la instalación del agente de GuardDuty está en buen estado. Para obtener más información, consulte [Validar el estado de instalación del agente de seguridad de GuardDuty](#).

Método 2: utilizar administradores de paquetes de Linux

Con este método, puede instalar el agente de seguridad de GuardDuty mediante la ejecución de scripts RPM o scripts Debian. En función de los sistemas operativos, puede elegir el método que prefiera:

- Utilice scripts RPM para instalar el agente de seguridad en las distribuciones de sistema operativo AL2, AL2023, RedHat, CentOS o Fedora.
- Utilice los scripts de Debian para instalar el agente de seguridad en las distribuciones de sistema operativo Ubuntu o Debian. Para obtener información sobre las distribuciones de Ubuntu y Debian compatibles, consulte [Validar los requisitos de arquitectura](#).

RPM installation

Important

Recomendamos que verifique la firma RPM del agente de seguridad de GuardDuty antes de instalarlo en la máquina.

1. Verifique la firma RPM del agente de seguridad de GuardDuty

a. Prepare la plantilla

Prepare los comandos con la clave pública adecuada, la firma del RPM x86_64, la firma del RPM arm64 y el enlace de acceso correspondiente a los scripts RPM alojados en buckets de Amazon S3. Sustituya el valor de la Región de AWS, el ID de la cuenta de AWS, y la versión del agente de GuardDuty para acceder a los scripts RPM.

- Clave pública:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/publickey.pem
```

- Firma RPM del agente de seguridad de GuardDuty:

Firma de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/x86_64/amazon-guardduty-agent-1.9.0.x86_64.sig
```

Firma de arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/arm64/amazon-guardduty-agent-1.9.0.arm64.sig
```

- Enlaces de acceso a los scripts RPM en el bucket de Amazon S:

Enlace de acceso para x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/x86_64/amazon-guardduty-agent-1.9.0.x86_64.rpm
```

Enlace de acceso para arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/arm64/amazon-guardduty-agent-1.9.0.arm64.rpm
```

Región de AWS	Nombre de la región	ID de la cuenta de AWS
eu-west-1	Europa (Irlanda)	694911143906

us-east-1	Este de EE. UU. (Norte de Virginia)	593207742271
us-west-2	Oeste de EE. UU. (Oregón)	733349766148
eu-west-3	Europa (París)	665651866788
us-east-2	Este de EE. UU. (Ohio)	307168627858
eu-central-1	Europa (Fráncfort)	323658145986
ap-northeast-2	Asia-Pacífico (Seúl)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Asia-Pacífico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Baréin)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Asia-Pacífico (Tokio)	533107202818
ap-southeast-1	Asia-Pacífico (Singapur)	174946120834
ap-south-1	Asia-Pacífico (Mumbai)	251508486986
ap-southeast-3	Asia-Pacífico (Yakarta)	510637619217
sa-east-1	América del Sur (São Paulo)	758426053663
ap-northeast-3	Asia-Pacífico (Osaka)	273192626886
eu-south-1	Europa (Milán)	266869475730
af-south-1	África (Ciudad del Cabo)	197869348890
ap-southeast-2	Asia-Pacífico (Sídney)	005257825471

me-central-1	Medio Oriente (EAU)	000014521398
us-west-1	Oeste de EE. UU. (Norte de California)	684579721401
ca-central-1	Canadá (centro)	354763396469
ca-west-1	Oeste de Canadá (Calgary)	339712888787
ap-south-2	Asia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (España)	919611009337
eu-central-2	Europa (Zúrich)	529164026651
ap-southeast-4	Asia-Pacífico (Melbourne)	251357961535
ap-southeast-7	Asia-Pacífico (Tailandia)	054037130133
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	México (central)	982081086614
ap-east-2	Asia-Pacífico (Taipei)	259886477082

b. Descargar la plantilla

En el siguiente comando para descargar la clave pública apropiada, la firma del RPM x86_64, la firma del RPM arm64 y el enlace de acceso correspondiente a los scripts RPM alojados en buckets de Amazon S3, asegúrese de sustituir el ID de cuenta por el ID de Cuenta de AWS apropiado y la región por la región actual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/
x86_64/amazon-guardduty-agent-1.9.0.x86_64.rpm ./amazon-guardduty-
agent-1.9.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/
x86_64/amazon-guardduty-agent-1.9.0.x86_64.sig ./amazon-guardduty-
agent-1.9.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.9.0/
publickey.pem ./publickey.pem
```

c. Importar la clave pública

Utilice el siguiente comando para importar la clave pública a la base de datos:

```
gpg --import publickey.pem
```

gpg muestra que la importación se realizó correctamente

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Verificación de la firma

Utilice el siguiente comando para verificar la firma

```
gpg --verify amazon-guardduty-agent-1.9.0.x86_64.sig amazon-guardduty-
agent-1.9.0.x86_64.rpm
```

Si aprueba la verificación, verá un mensaje similar al resultado que se muestra a continuación. Ahora puede proceder a instalar el agente de seguridad de GuardDuty mediante RPM.

Ejemplo de salida:

```
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
```

Si la verificación falla, significa que la firma en RPM ha sido potencialmente manipulada. Debe eliminar la clave pública de la base de datos e intentar de nuevo el proceso de verificación.

Ejemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
```

```
gpg: BAD signature from "AwsGuardDuty"
```

Utilice el siguiente comando para eliminar la clave pública de la base de datos:

```
gpg --delete-keys AwsGuardDuty
```

Ahora, intente de nuevo el proceso de verificación.

2. [Conéctese con SSH desde Linux o macOS.](#)
3. Instale el agente de seguridad de GuardDuty mediante el siguiente comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.9.0.x86_64.rpm
```

4. Valide si la instalación del agente de GuardDuty está en buen estado. Para obtener más información sobre los pasos, consulte [Validar el estado de instalación del agente de seguridad de GuardDuty](#).

Debian installation

Important

Recomendamos que verifique la firma de Debian del agente de seguridad de GuardDuty antes de instalarlo en la máquina.

1. Verifique la firma de Debian del agente de seguridad de GuardDuty
 - a. Prepare plantillas para la clave pública adecuada, la firma del paquete de Debian amd64, la firma del paquete de Debian arm64 y el enlace de acceso correspondiente a los scripts de Debian alojados en buckets de Amazon S3.

En las siguientes plantillas, sustituya el valor del Región de AWS, el ID de la cuenta de AWS y la versión del agente de GuardDuty para acceder a los scripts de paquetes Debian.

- Clave pública:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/  
publickey.pem
```

- Firma de Debian del agente de seguridad GuardDuty:

Firma de amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/amd64/
amazon-guardduty-agent-1.9.0.amd64.sig
```

Firma de arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/arm64/
amazon-guardduty-agent-1.9.0.arm64.sig
```

- Enlaces de acceso a los scripts Debian en el bucket de Amazon S:

Enlace de acceso para amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/amd64/
amazon-guardduty-agent-1.9.0.amd64.deb
```

Enlace de acceso para arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/arm64/
amazon-guardduty-agent-1.9.0.arm64.deb
```

Región de AWS	Nombre de la región	ID de la cuenta de AWS
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Este de EE. UU. (Norte de Virginia)	593207742271
us-west-2	Oeste de EE. UU. (Oregón)	733349766148
eu-west-3	Europa (París)	665651866788
us-east-2	Este de EE. UU. (Ohio)	307168627858
eu-central-1	Europa (Fráncfort)	323658145986

ap-northeast-2	Asia-Pacífico (Seúl)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Asia-Pacífico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Baréin)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Asia-Pacífico (Tokio)	533107202818
ap-southeast-1	Asia-Pacífico (Singapur)	174946120834
ap-south-1	Asia-Pacífico (Mumbai)	251508486986
ap-southeast-3	Asia-Pacífico (Yakarta)	510637619217
sa-east-1	América del Sur (São Paulo)	758426053663
ap-northeast-3	Asia-Pacífico (Osaka)	273192626886
eu-south-1	Europa (Milán)	266869475730
af-south-1	África (Ciudad del Cabo)	197869348890
ap-southeast-2	Asia-Pacífico (Sídney)	005257825471
me-central-1	Medio Oriente (EAU)	000014521398
us-west-1	Oeste de EE. UU. (Norte de California)	684579721401
ca-central-1	Canadá (centro)	354763396469
ca-west-1	Oeste de Canadá (Calgary)	339712888787
ap-south-2	Asia-Pacífico (Hyderabad)	950823858135

eu-south-2	Europa (España)	919611009337
eu-central-2	Europa (Zúrich)	529164026651
ap-southeast-4	Asia-Pacífico (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	México (central)	982081086614
ap-east-2	Asia-Pacífico (Taipéi)	259886477082

- b. Descargue la clave pública adecuada, la firma de amd64, la firma de arm64 y el enlace de acceso correspondiente a los scripts de Debian alojados en los buckets de Amazon S3

En los siguientes comandos, sustituya el ID de cuenta por el ID de Cuenta de AWS adecuado y la región por la región actual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/
amd64/amazon-guardduty-agent-1.9.0.amd64.deb ./amazon-guardduty-
agent-1.9.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/
amd64/amazon-guardduty-agent-1.9.0.amd64.sig ./amazon-guardduty-
agent-1.9.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.9.0/
publickey.pem ./publickey.pem
```

- c. Importar la clave pública a la base de datos

```
gpg --import publickey.pem
```

gpg muestra que la importación se realizó correctamente

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

- d. Verificación de la firma

```
gpg --verify amazon-guardduty-agent-1.9.0.amd64.sig amazon-guardduty-agent-1.9.0.amd64.deb
```

Tras una verificación correcta, verá un mensaje similar al siguiente resultado:

Ejemplo de salida:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
gpg:          owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Ahora puede proceder a instalar el agente de seguridad de GuardDuty mediante Debian.

Sin embargo, si se produce un error en la verificación, significa que la firma en el paquete Debian ha sido potencialmente manipulada.

Ejemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Utilice el siguiente comando para eliminar la clave pública de la base de datos:

```
gpg --delete-keys AwsGuardDuty
```

Ahora, intente de nuevo el proceso de verificación.

2. [Conéctese con SSH desde Linux o macOS.](#)
3. Instale el agente de seguridad de GuardDuty mediante el siguiente comando:

```
sudo dpkg -i amazon-guardduty-agent-1.9.0.amd64.deb
```

4. Valide si la instalación del agente de GuardDuty está en buen estado. Para obtener más información sobre los pasos, consulte [Validar el estado de instalación del agente de seguridad de GuardDuty](#).

Error de falta de memoria

Si se produce un error out-of-memory al instalar o actualizar manualmente el agente de seguridad de GuardDuty para Amazon EC2, consulte [Solución de problemas de memoria insuficiente](#).

Validar el estado de instalación del agente de seguridad de GuardDuty

Después de haber seguido los pasos para instalar el agente de seguridad de GuardDuty, siga los siguientes pasos para validar el estado del agente:

Para validar si el agente de seguridad GuardDuty está en buen estado

1. [Conéctese con SSH desde Linux o macOS](#).
2. Ejecute el siguiente comando para comprobar el estado del agente de seguridad de GuardDuty:

```
sudo systemctl status amazon-guardduty-agent
```

Si desea ver los registros de instalación del agente de seguridad, están disponibles en `/var/log/amzn-guardduty-agent/`.

Para ver los registros, realice `sudo journalctl -u amazon-guardduty-agent`.

Actualizar manualmente el agente de seguridad de GuardDuty para una instancia de Amazon EC2

GuardDuty lanza actualizaciones de las versiones de los agentes de seguridad. Si administra el agente de seguridad manualmente, es responsable de actualizar el agente para las instancias de Amazon EC2. Para obtener información sobre las nuevas versiones de los agentes, consulte [Versiones del agente de seguridad de GuardDuty](#) para las instancias de Amazon EC2. Para recibir notificaciones sobre el lanzamiento de una nueva versión del agente, consulte [Suscripción a los anuncios de Amazon SNS para GuardDuty](#).

Para actualizar manualmente el agente de seguridad para una instancia de Amazon EC

El proceso para actualizar el agente de seguridad es el mismo que para instalarlo. Según el método que haya utilizado para instalar el agente, puede seguir los pasos que se indican en [Instalación manual del agente de seguridad](#) para las instancias de Amazon EC2.

Si utiliza el [Método 1: mediante AWS Systems Manager](#), puede actualizar el agente de seguridad mediante el Comando de ejecución. Utilice la versión del agente a la que desea actualizar.

Si utiliza el [Método 2: mediante administradores de paquetes de Linux](#), puede usar los scripts tal como se indica en la sección [Instalación manual del agente de seguridad](#). Los scripts ya incluyen la versión más reciente del agente. Para obtener información sobre las versiones de agentes lanzadas recientemente, consulte [Versiones del agente de seguridad de GuardDuty para instancias de Amazon EC2](#).

Después de actualizar el agente de seguridad, puede comprobar el estado de la instalación al consultar los registros. Para obtener más información, consulte [Validar el estado de instalación del agente de seguridad de GuardDuty](#).

Administrar el agente de seguridad automatizado para Fargate (solo Amazon ECS)

La supervisión en tiempo de ejecución permite administrar el agente de seguridad de los clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Antes de continuar con los pasos de esta sección, asegúrese de cumplir con [Requisitos previos para la compatibilidad con AWS Fargate \(solo con Amazon ECS\)](#).

En función de [Enfoques al administrar el agente de seguridad de GuardDuty en los recursos de Amazon ECS-Fargate](#), elija el método que prefiera para habilitar el agente automatizado GuardDuty para los recursos.

Configurar el agente de GuardDuty para un entorno de varias cuentas

En un entorno de varias cuentas, solo la cuenta de administrador delegado de GuardDuty puede habilitar o desactivar la configuración automatizada de agentes para las cuentas de miembro y administrar la configuración automatizada de agentes para los clústeres de Amazon ECS que pertenezcan a las cuentas de miembro en la organización. Una cuenta de miembro de GuardDuty no puede modificar esta configuración. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro mediante AWS Organizations. Para obtener más información sobre los entornos con varias cuentas, consulte [Administrar varias cuentas en GuardDuty](#).

Habilitar la configuración automatizada de agentes para la cuenta de administrador delegado de GuardDuty

Manage for all Amazon ECS clusters (account level)

Si ha elegido Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución, tendrá las siguientes opciones:

- Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente. GuardDuty implementará y administrará el agente de seguridad para todas las tareas de Amazon ECS que se lancen.
- Elija Configurar cuentas manualmente.

Si ha elegido Configurar cuentas manualmente en la sección Supervisión en tiempo de ejecución, haga lo siguiente:

1. Elija Configurar cuentas manualmente en la sección Configuración automatizada del agente.
2. Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta).

Seleccione Save.

Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como `GuardDutyManaged=false`.

2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.

5.

 Note

Agregue siempre la etiqueta de exclusión a los clústeres de Amazon ECS antes de habilitar la configuración automatizada del agente para su cuenta; de lo contrario, el contenedor sidecar de GuardDuty se asociará a todos los contenedores en las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, elija Habilitar en la Configuración automatizada del agente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty administrará la implementación del agente de seguridad en el contenedor sidecar.

6. Seleccione Save.

7. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser `GuardDutyManaged=true`.
2. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar el agente de GuardDuty a través de la configuración automatizada del agente de forma explícita.

3. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución.

Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Habilitar automáticamente para todas las cuentas de miembro

Manage for all Amazon ECS clusters (account level)

Los siguientes pasos presuponen que ha elegido Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución.

1. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente. GuardDuty implementará y administrará el agente de seguridad para todas las tareas de Amazon ECS que se lancen.
2. Seleccione Save.
3. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged-false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

4. En el panel de navegación, elija Supervisión en tiempo de ejecución.

- 5.

 Note

Agregue siempre la etiqueta de exclusión a los clústeres de Amazon ECS antes de habilitar la configuración automatizada del agente para su cuenta; de lo contrario, el contenedor sidecar de GuardDuty se asociará a todos los contenedores en las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, elija Editar.

6. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty administrará la implementación del agente de seguridad en el contenedor sidecar.

7. Seleccione Save.
8. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Independientemente de cómo decida habilitar la Supervisión en tiempo de ejecución, los pasos que se indican a continuación sirven para supervisar tareas específicas de Amazon ECS Fargate para todas las cuentas de miembro de la organización.

1. No habilite ninguna configuración en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que seleccionó en el paso anterior.

2. Seleccione Save.
3. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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

Cuando se utilizan etiquetas de inclusión para los clústeres de Amazon ECS, no es necesario habilitar explícitamente la administración automática de agentes de GuardDuty.

4. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Habilitar la configuración automática del agente para las cuentas de miembro activas existentes

Manage for all Amazon ECS clusters (account level)

1. En la página Supervisión del tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración automatizada del agente.
2. En el panel de configuración automática de agentes, en la sección Cuentas de miembros activos, seleccione Acciones.
3. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
4. Elija Confirmar.
5. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged-false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 Note

Agregue siempre la etiqueta de exclusión a los clústeres de Amazon ECS antes de habilitar la configuración automatizada del agente para su cuenta; de lo contrario, el contenedor sidecar de GuardDuty se asociará a todos los contenedores en las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, en la sección Configuración automatizada del agente, en Cuentas de miembro activas, elija Acciones.

6. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty administrará la implementación del agente de seguridad en el contenedor sidecar.

7. Elija Confirmar.
8. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
2. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar la Configuración automatizada del agente de forma explícita.

3. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Habilitar automáticamente la configuración automática de agentes para los nuevos miembros

Manage for all Amazon ECS clusters (account level)

1. En la página Supervisión en tiempo de ejecución, elija Editar para actualizar la configuración existente.
2. En la sección Configuración automatizada del agente, seleccione Habilitar automáticamente para nuevas cuentas de miembro.
3. Seleccione Save.
4. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged-false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 Note

Agregue siempre la etiqueta de exclusión a los clústeres de Amazon ECS antes de habilitar la configuración automatizada del agente para su cuenta; de lo contrario, el contenedor sidecar de GuardDuty se asociará a todos los contenedores en las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, seleccione Habilitar automáticamente para nuevas cuentas de miembro en la sección Configuración automatizada del agente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty administrará la implementación del agente de seguridad en el contenedor sidecar.

6. Seleccione Save.
7. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
2. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar la Configuración automatizada del agente de forma explícita.

3. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Habilitar la Configuración automatizada del agente para cuentas de miembro activas de forma selectiva

Manage for all Amazon ECS (account level)

1. En la página Cuentas, seleccione las cuentas para las que desea habilitar la Configuración automatizada del agente de la Supervisión en tiempo de ejecución (ECS-Fargate). Puede seleccionar varias cuentas. Asegúrese de que las cuentas que seleccione en este paso ya estén habilitadas con la Supervisión en tiempo de ejecución.
2. En Editar planes de protección, elija la opción adecuada para habilitar la Configuración automatizada del agente de la Supervisión en tiempo de ejecución (ECS-Fargate).
3. Elija Confirmar.
4. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged-false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 Note

Siempre agregue la etiqueta de exclusión a los clústeres de Amazon ECS antes de habilitar la administración automatizada del agente de GuardDuty para la cuenta; de lo contrario, el contenedor sidecar de GuardDuty se asociará a todos los contenedores en las tareas de Amazon ECS que se lancen.

En la página Cuentas, seleccione las cuentas para las que desea habilitar la Configuración automatizada del agente de la Supervisión en tiempo de ejecución (ECS-Fargate). Puede seleccionar varias cuentas. Asegúrese de que las cuentas que seleccione en este paso ya estén habilitadas con la Supervisión en tiempo de ejecución.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty administrará la implementación del agente de seguridad en el contenedor sidecar.

6. En Editar planes de protección, elija la opción adecuada para habilitar la Configuración automatizada del agente de la Supervisión en tiempo de ejecución (ECS-Fargate).
7. Seleccione Save.
8. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.

- [update-service](#) en la Referencia del comando de la AWS CLI.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Asegúrese de no habilitar la Configuración automatizada del agente (o Configuración automatizada del agente de Supervisión en tiempo de ejecución [ECS-Fargate]) para las cuentas seleccionadas que tienen los clústeres de Amazon ECS que desea supervisar.
2. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
3. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar la Configuración automatizada del agente de forma explícita.

4. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Configurar el agente de GuardDuty para una cuenta independiente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración:
 - a. Para administrar la Configuración automatizada del agente para todos los clústeres de Amazon ECS (nivel de cuenta)

Elija Habilitar en la sección Configuración automatizada del agente para AWS Fargate (sólo ECS). Cuando se lanza una nueva tarea de Amazon ECS de Fargate, GuardDuty administrará la implementación del agente de seguridad.

- Seleccione Save.

- b. Para administrar la Configuración automatizada del agente mediante la exclusión de algunos de los clústeres de Amazon ECS (nivel de clúster)
 - i. Agregue una etiqueta al clúster de Amazon ECS para el que desea excluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged-false.
 - ii. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

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. En la pestaña Configuración, elija Habilitar en la sección Configuración automatizada del agente.

 Note

Siempre agregue la etiqueta de exclusión al clúster de Amazon ECS antes de habilitar la administración automática del agente de GuardDuty para la cuenta; de lo contrario, el agente de seguridad se implementará en todas las tareas que se lancen dentro del clúster de Amazon ECS correspondiente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty administrará la implementación del agente de seguridad en el contenedor sidecar.

- iv. Seleccione Save.
- c. Para administrar la Configuración automatizada del agente mediante la inclusión de algunos de los clústeres de Amazon ECS (nivel de clúster).
 - i. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
 - ii. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringNotEquals": {
        "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
      }
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],

```

```
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn":
          "arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
}
```

4. Si desea que GuardDuty supervise tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar la Supervisión en tiempo de ejecución. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la Referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI.

Administración automática del agente de seguridad para los recursos de Amazon EKS

La Supervisión en tiempo de ejecución permite habilitar el agente de seguridad tanto mediante la configuración automatizada de GuardDuty como manualmente. En esta sección se indican los pasos necesarios para habilitar la configuración automatizada del agente para los clústeres de Amazon EKS.

Antes de continuar, asegúrese de haber cumplido con los [Requisitos previos para la compatibilidad con clústeres de Amazon EKS](#).

Según el enfoque que prefiera para [Administración del agente de seguridad a través de GuardDuty](#), elija los pasos a seguir en las próximas secciones en consecuencia.

Configuración automatizada del agente para entornos de varias cuentas

En entornos de varias cuentas, solo la cuenta de administrador delegado de GuardDuty puede habilitar o desactivar la Configuración automatizada del agente para las cuentas de miembro, y administrar el agente automatizado para los clústeres de EKS que pertenezcan a las cuentas de miembro de la organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro a través de AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

Ajustar la Configuración automatizada del agente para la cuenta de administrador delegado de GuardDuty

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (Supervisión de todos los clústeres de EKS)	Si eligió Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución, dispondrá de las siguientes opciones: • Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente. GuardDuty implementará y administrará el agente de seguridad para todos los clústeres de EKS que pertenezcan a la cuenta de administrador delegado de GuardDuty y también para todos los clústeres de EKS que pertenezcan a todas las cuentas de miembro existentes y potencialmente nuevas en la organización. • Elija Configurar cuentas manualmente. Si ha elegido Configurar cuentas manualmente en la sección Supervisión en tiempo de ejecución, haga lo siguiente: 1. Elija Configurar cuentas manualmente en la sección Configuración automatizada del agente.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	2. Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta). Seleccione Save.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty no se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> . • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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> 3. Abra la consola de GuardDuty en https://console.aws.amazon.com/guardduty/.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	4. En el panel de navegación, elija Supervisión en tiempo de ejecución.  Note Agregue siempre la etiqueta de exclusión a sus clústeres de EKS antes de habilitar la administración automática del agente de GuardDuty en su cuenta; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta. 5. En la pestaña Configuración, elija Habilitar en la sección Administración del agente de GuardDuty. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty administrará la implementación y las actualizaciones del agente de seguridad de GuardDuty. 6. Seleccione Save. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes:

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> . • Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> . • Sustituya <i>access-project</i> por <code>GuardDutyManaged</code> . • Sustituya <i>123456789012</i> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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> 3. Si tenía habilitado el agente automatizado para este clúster de EKS, después de este paso, GuardDuty no actualizará el agente de seguridad para este clúster. Sin embargo, el agente de seguridad seguirá implementado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución . 4. Si administraba manualmente el agente de seguridad de GuardDuty para este clúster de EKS, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultarán útiles a la hora de supervisar determinados clústeres de EKS en la cuenta: 1. Asegúrese de elegir Desactivar para la cuenta de administrador delegado de GuardDuty (esta cuenta) en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. 2. Seleccione Save. 3. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para determinados clústeres de EKS que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code>:

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<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>
Administración manual del agente de seguridad de GuardDuty	Independientemente de cómo haya decidido habilitar la supervisión en tiempo de ejecución, puede administrar el agente de seguridad manualmente para los clústeres de EKS. 1. Asegúrese de elegir Desactivar para la cuenta de administrador delegado de GuardDuty (esta cuenta) en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. 2. Seleccione Save. 3. Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Habilitar automáticamente el agente automatizado para todas las cuentas de miembro

 Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (Supervisión de todos los clústeres de EKS)	Este tema es para habilitar la Supervisión en tiempo de ejecución para todas las cuentas de miembro y, por lo tanto, los siguientes pasos suponen que la opción Habilitar para todas las cuentas se ha elegido en la sección Supervisión en tiempo de ejecución. 1. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente. GuardDuty implementará y administrará el agente de seguridad para todos los clústeres de EKS que pertenezcan a la cuenta de administrador delegado de GuardDuty y también para todos los clústeres de EKS que pertenezcan a todas las cuentas de miembro existentes y potencialmente nuevas en la organización. 2. Seleccione Save.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty no se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya <i>access-project</i> por GuardDutyManaged . • Sustituya <i>123456789012</i> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de 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. Abra la consola de GuardDuty en https://console.aws.amazon.com/guardduty/. 4. En el panel de navegación, elija Supervisión en tiempo de ejecución.  Note Siempre agregue la etiqueta de exclusión a los clústeres de EKS antes de habilitar el agente automatizado para la cuenta; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS en la cuenta. 5. En la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución. 6. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty administrará la implementación y las actualizaciones del agente de seguridad de GuardDuty. 7. Seleccione Save.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Si tenía habilitada la Configuración automatizada del agente para este clúster de EKS, después de este paso, GuardDuty no actualizará el agente de seguridad para este clúster. Sin embargo, el agente de seguridad seguirá implementado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución. 3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> .

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya 123456789012 por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de 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> 4. Si administraba manualmente el agente de seguridad de GuardDuty para este clúster de EKS, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultan útiles a la hora de supervisar determinados clústeres de EKS para todas las cuentas de miembros en la organización: 1. No habilite ninguna configuración en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. 2. Seleccione Save. 3. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para determinados clústeres de EKS que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code>:

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<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>
Administración manual del agente de seguridad de GuardDuty	Independientemente de cómo haya decidido habilitar la supervisión en tiempo de ejecución, puede administrar el agente de seguridad manualmente para los clústeres de EKS. 1. No habilite ninguna configuración en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. 2. Seleccione Save. 3. Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Habilitar el agente automatizado para todas las cuentas de miembro activas existentes

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Administración del agente de seguridad de GuardDuty para las cuentas de miembros activas existentes de la organización

- Para que GuardDuty reciba los eventos de tiempo de ejecución de los clústeres de EKS que pertenecen a las cuentas de miembros activas existentes de la organización, debe elegir el enfoque que prefiera para administrar el agente de seguridad de GuardDuty para estos clústeres de EKS. Para obtener más información acerca de cada uno de estos métodos,

consulte [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#).

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (Supervisión de todos los clústeres de EKS)	Supervisión de todos los clústeres de EKS para todas las cuentas de miembros activas existentes 1. En la página Supervisión del tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración automatizada del agente. 2. En el panel Configuración automatizada del agente, en la sección Cuentas de miembro activas, seleccione Acciones. 3. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes. 4. Elija Confirmar.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty no se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> : <pre data-bbox="805 495 1398 726">"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. Abra la consola de GuardDuty en https://console.aws.amazon.com/guardduty/. 4. En el panel de navegación, elija Supervisión en tiempo de ejecución.  Note Siempre agregue la etiqueta de exclusión a los clústeres de EKS antes de habilitar la configuración automatizada del agente para la cuenta; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS en la cuenta. 5. En la pestaña Configuración, en la sección Configuración automatizada del agente, en Cuentas de miembro activas, elija Acciones. 6. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas. 7. Elija Confirmar.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Exclusión de un clúster de EKS de la supervisión una vez implementado el agente de seguridad de GuardDuty en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Tras este paso, GuardDuty no actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad seguirá implementado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya 123456789012 por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de 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. Independientemente de cómo administre el agente de seguridad (mediante GuardDuty o manualmente), para dejar de recibir los eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado desde este clúster de EKS. Para obtener más información acerca de la eliminación del agente de seguridad implementado, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	1. En la página Cuentas, después de habilitar la Supervisión en tiempo de ejecución, no habilite Supervisión en tiempo de ejecución: configuración automatizada del agente. 2. Agregue una etiqueta al clúster de EKS que pertenezca a la cuenta seleccionada que desee supervisar. El par de clave-valor de la etiqueta debe ser <code>GuardDutyManaged -true</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para determinados clústeres de EKS que desee supervisar. 3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Sustituya 123456789012 por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de 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>
Administración manual del agente de seguridad de GuardDuty	- Asegúrese de no elegir Habilitar en la sección Configuración automatizada del agente. Mantenga habilitada la Supervisión en tiempo de ejecución. - Seleccione Save. - Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Habilitar automáticamente la configuración automatizada del agente para los nuevos miembros

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (Supervisión de todos los clústeres de EKS)	- En la página Supervisión en tiempo de ejecución, elija Editar para actualizar la configuración existente. - En la sección Configuración automatizada del agente, seleccione Habilitar automáticamente para nuevas cuentas de miembro.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3. Seleccione Save.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty no se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> : <pre data-bbox="748 474 1507 709">"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> - Abra la consola de GuardDuty en https://console.aws.amazon.com/guardduty/. - En el panel de navegación, elija Supervisión en tiempo de ejecución.  Note Siempre agregue la etiqueta de exclusión a los clústeres de EKS antes de habilitar la configuración automatizada del agente para la cuenta; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS en la cuenta. - En la pestaña Configuración, seleccione Habilitar automáticamente para las cuentas de nuevos miembros en la sección Administración del agente de GuardDuty. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty administrará la implementación y las actualizaciones del agente de seguridad de GuardDuty. - Seleccione Save.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty se ha implementado en este clúster 1. Independientemente de si administra el agente de seguridad de GuardDuty a través de GuardDuty o manualmente, agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Si tenía habilitado el agente automatizado para este clúster de EKS, después de este paso, GuardDuty no actualizará el agente de seguridad para este clúster. Sin embargo, el agente de seguridad seguirá implementado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> . • Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> . • Sustituya <i>access-project</i> por <code>GuardDutyManaged</code> . • Sustituya <i>123456789012</i> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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> 3. Si administraba manualmente el agente de seguridad de GuardDuty para este clúster de EKS, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultan útiles a la hora de supervisar determinados clústeres de EKS para las nuevas cuentas de miembro en la organización. 1. Asegúrese de desmarcar Habilitar automáticamente para nuevas cuentas de miembro en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. 2. Seleccione Save. 3. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para determinados clústeres de EKS que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> . • Sustituya <i>access-project</i> por <code>GuardDutyManaged</code> . • Sustituya <i>123456789012</i> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>
Administración manual del agente de seguridad de GuardDuty	Independientemente de cómo haya decidido habilitar la supervisión en tiempo de ejecución, puede administrar el agente de seguridad manualmente para los clústeres de EKS. 1. Asegúrese de desmarcar la casilla Habilitar automáticamente para nuevas cuentas de miembro en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. 2. Seleccione Save. 3. Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Configurar el agente automatizado para cuentas de miembro activas de forma selectiva

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (Supervisión de todos los clústeres de EKS)	1. En la página Cuentas, seleccione las cuentas para las que desea activar la Configuración automatizada del agente. Puede seleccionar más de una cuenta a la vez. Asegúrese de que las cuentas que seleccione en este paso ya tengan habilitada la supervisión en tiempo de ejecución de EKS. 2. En Editar planes de protección, elija la opción adecuada para habilitar la Supervisión en tiempo de ejecución: configuración automatizada del agente. 3. Elija Confirmar.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty no se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> .

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya 123456789012 por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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> - Abra la consola de GuardDuty en https://console.aws.amazon.com/guardduty/.  Note Siempre agregue la etiqueta de exclusión a los clústeres de EKS antes de habilitar la configuración automatizada del agente para la cuenta; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS en la cuenta. - En la página Cuentas, seleccione la cuenta para la que desee habilitar Administrar agente automáticamente. Puede seleccionar más de una cuenta a la vez. - En Editar planes de protección, elija la opción adecuada para habilitar la Supervisión en tiempo de ejecución: configuración automatizada del agente para la cuenta seleccionada. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty administrará la implementación y las actualizaciones del agente de seguridad de GuardDuty. - Seleccione Save.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty se ha implementado en este clúster Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Si previamente tenía habilitada la Configuración automatizada del agente para este clúster de EKS, después de este paso, GuardDuty no actualizará el agente de seguridad para este clúster. Sin embargo, el agente de seguridad seguirá implementado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: - Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. - Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. - Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	• Sustituya 123456789012 por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de 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. Si administraba manualmente el agente de seguridad de GuardDuty para este clúster de EKS, debe eliminarlo. Para obtener más información, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultan útiles a la hora de supervisar determinados clústeres de EKS que pertenecen a las cuentas seleccionadas: 1. Asegúrese de no habilitar Supervisión en tiempo de ejecución : configuración automatizada del agente para las cuentas seleccionadas en las que se encuentran los clústeres de EKS que desea supervisar. 2. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Tras agregar la etiqueta, GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para determinados clústeres de EKS que desee supervisar. 3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> . • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre data-bbox="639 323 1406 474">"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>
Administración manual del agente de seguridad de GuardDuty	1. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. Asegúrese de no habilitar Supervisión en tiempo de ejecución: configuración automatizada del agente para ninguna de las cuentas seleccionadas. 2. Elija Confirmar. 3. Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Configurar el agente automatizado para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#).

Después de habilitar la Supervisión en tiempo de ejecución, asegúrese de instalar el agente de seguridad de GuardDuty mediante una configuración automática o una implementación manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Según su preferencia de supervisar todos o algunos recursos de Amazon EKS, elija el método que prefiera y siga los pasos que se indican en la tabla siguiente.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, elija Habilitar para habilitar la configuración automatizada del agente para la cuenta.

Método preferido para implementar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (Supervisión de todos los clústeres de EKS)	1. Elija Habilitar en la sección Configuración automatizada del agente. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de EKS existentes y potencialmente nuevos de su cuenta. 2. Seleccione Save.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que le corresponda. Exclusión de un clúster de EKS de la supervisión cuando el agente de seguridad de GuardDuty no se ha implementado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como GuardDutyManaged y su valor como false. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en

Método preferido para implementar el agente de seguridad de GuardDuty	Pasos
	la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> . • Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> . • Sustituya <i>access-project</i> por <code>GuardDutyManaged</code> . • Sustituya <i>123456789012</i> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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> 3. Abra la consola de GuardDuty en https://console.aws.amazon.com/guardduty/. 4. En el panel de navegación, elija Supervisión en tiempo de ejecución.  Note Agregue siempre la etiqueta de exclusión a sus clústeres de EKS antes de habilitar la administración automática del agente de GuardDuty en su cuenta; de lo contrario,

Método preferido para implementar el agente de seguridad de GuardDuty	Pasos
	el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta. 5. En la pestaña Configuración, elija Habilitar en la sección Administración del agente de GuardDuty. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty administrará la implementación y las actualizaciones del agente de seguridad de GuardDuty. 6. Seleccione Save. Exclusión de un clúster de EKS de la supervisión una vez implementado el agente de seguridad de GuardDuty en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Tras este paso, GuardDuty no actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad seguirá implementado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.

Método preferido para implementar el agente de seguridad de GuardDuty	Pasos
	2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code>. • Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code>. • Sustituya <i>access-project</i> por <code>GuardDutyManaged</code>. • Sustituya <i>123456789012</i> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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> 3. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información acerca de la eliminación del agente de seguridad implementado, consulte Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución.

Método preferido para implementar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	1. Asegúrese de no elegir Desactivar en la sección Configuración automatizada del agente. Mantenga habilitada la Supervisión en tiempo de ejecución. 2. Seleccione Guardar. 3. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para determinados clústeres de EKS que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2>DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza.

Método preferido para implementar el agente de seguridad de GuardDuty	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> : <pre data-bbox="803 493 1396 724">"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>
Administración manual del agente	1. Asegúrese de no elegir Desactivar en la sección Configuración automatizada del agente. Mantenga habilitada la Supervisión en tiempo de ejecución. 2. Seleccione Save. 3. Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Administrar manualmente el agente de seguridad para el clúster de Amazon EKS

En esta sección se describe cómo puede administrar el agente complemento de Amazon EKS (agente de GuardDuty) después de habilitar la Supervisión en tiempo de ejecución (o la Supervisión en tiempo de ejecución de EKS). Para utilizar la Supervisión en tiempo de ejecución, debe habilitarla y configurar el complemento de Amazon EKS, `aws-guardduty-agent`. Debe seguir ambos pasos para que GuardDuty detecte amenazas potenciales y genere [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#).

Para administrar el agente manualmente, es necesario crear un punto de conexión VPC como requisito previo. Esto ayuda a GuardDuty a recibir los eventos en tiempo de ejecución. Después de esto, podrá instalar el agente de seguridad para que GuardDuty comience a recibir los eventos en

tiempo de ejecución de los recursos de Amazon EKS. Cuando GuardDuty lanza una nueva versión de agente para este recurso, se puede actualizar la versión del agente en la cuenta.

Temas

- [Requisito previo: crear un punto de conexión de Amazon VPC](#)
- [Instalar manualmente el agente de seguridad de GuardDuty en los recursos de Amazon EKS](#)
- [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#)

Requisito previo: crear un punto de conexión de Amazon VPC

Antes de poder instalar el agente de seguridad GuardDuty, debe crear un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC). Esto ayudará a GuardDuty a recibir los eventos en tiempo de ejecución de los recursos de Amazon EKS.

Note

El uso del punto de conexión de VPC no conlleva ningún costo adicional.

Elija el método de acceso que prefiera para crear un punto de conexión de Amazon VPC.

Console

Para crear un punto de conexión de VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, en Nube virtual privada, seleccione Puntos de conexión.
3. Seleccione Crear punto de conexión.
4. En la página Crear punto de conexión, en Categoría de servicio, elija Otros servicios de punto de conexión.
5. En Nombre del servicio, escriba **com.amazonaws.us-east-1.guardduty-data**.

Asegúrese de sustituir **us-east-1** por la región correcta. Debe ser la misma región que la del clúster de EKS que pertenece al ID de su Cuenta de AWS.

6. Elija Verificar el servicio.
7. Una vez que el nombre del servicio se haya verificado correctamente, elija la VPC en la que reside el clúster. Agregue la siguiente política para restringir el uso de los puntos de conexión

de VPC únicamente a la cuenta especificada. Con el valor de `Condition` de la organización que se indica debajo de esta política, puede actualizar la siguiente política para restringir el acceso a su punto de conexión. Para proporcionar compatibilidad con puntos de conexión de VPC a ID de cuentas específicos de su organización, consulte [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": "*"
    }
  ]
}
```

El ID de cuenta de `aws:PrincipalAccount` debe coincidir con la cuenta que contiene la VPC y el punto de conexión de VPC. En la siguiente lista se muestra cómo compartir el punto de conexión de VPC con otros ID de Cuenta de AWS:

Condición de la organización para restringir el acceso a su punto de conexión

- Si quiere especificar varias cuentas para acceder al punto de conexión de VPC, sustituya `"aws:PrincipalAccount": "111122223333"` por lo siguiente:

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

- Para permitir que todos los miembros de una organización accedan al punto de conexión de VPC, sustituya "aws:PrincipalAccount": "111122223333" por lo siguiente:

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

- Para restringir el acceso a un recurso a un ID de organización, agregue su ResourceOrgID a la política.

Para obtener más información, consulte [ResourceOrgID](#).

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

8. En Configuración adicional, seleccione Habilitar nombre de DNS.
9. En Subredes, elija las subredes en las que reside el clúster.
10. En Grupos de seguridad, elija un grupo de seguridad que tenga el puerto de entrada 443 habilitado desde su VPC (o su clúster de EKS). Si aún no tiene ningún grupo de seguridad que tenga habilitado el puerto de entrada 443, [cree un grupo de seguridad](#).

Si se produce un problema al restringir los permisos de entrada a la VPC (o instancia), puede utilizar el puerto de entrada 443 desde cualquier dirección IP (0.0.0.0/0). Sin embargo, GuardDuty recomienda utilizar direcciones IP que coincidan con el bloque de CIDR correspondiente a la VPC. Para obtener más información, consulte [Bloques de CIDR de VPC](#) en la Guía del usuario de Amazon VPC.

API/CLI

Para crear un punto de conexión de VPC

- Invoque [CreateVpcEndpoint](#).
- Utilice los siguientes valores para los parámetros:
 - En Nombre del servicio, escriba **com.amazonaws.us-east-1.guardduty-data**.

Asegúrese de sustituir *us-east-1* por la región correcta. Debe ser la misma región que la del clúster de EKS que pertenece al ID de su Cuenta de AWS.

- Para [DNSOptions](#), establezca la opción de DNS privado en `true` para habilitarla.
- Para AWS Command Line Interface, consulte [create-vpc-endpoint](#).

Una vez que haya seguido los pasos, consulte [Validar la configuración del punto de conexión de VPC](#) para asegurarse de que el punto de conexión de VPC se configuró correctamente.

Instalar manualmente el agente de seguridad de GuardDuty en los recursos de Amazon EKS

En esta sección se describe cómo puede implementar el agente de seguridad de GuardDuty por primera vez en clústeres de EKS específicos. Antes de continuar con esta sección, asegúrese de que ya ha configurado los requisitos previos y habilitado la Supervisión en tiempo de ejecución para las cuentas. El agente de seguridad de GuardDuty (complemento de EKS) no funcionará si no habilita la supervisión en tiempo de ejecución.

Elija el método de acceso que prefiera para implementar el agente de seguridad de GuardDuty por primera vez.

Console

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. Elija un nombre para el clúster.
3. Elija la pestaña Complementos.
4. Escoja Obtener más complementos.
5. En la página Seleccionar complementos, seleccione Supervisión en tiempo de ejecución de EKS en Amazon GuardDuty.
6. GuardDuty recomienda elegir la versión de agente más reciente y predeterminada.
7. En la página Definir configuración del complemento seleccionado, utilice la configuración predeterminada. Si el estado del complemento de EKS es Requiere activación, seleccione Activar GuardDuty. Esta acción abrirá la consola de GuardDuty para configurar la Supervisión en tiempo de ejecución para las cuentas.

8. Una vez que haya configurado la Supervisión en tiempo de ejecución para las cuentas, vuelva a la consola de Amazon EKS. El estado de su complemento de EKS debería haber cambiado a Listo para instalar.
9. (Opcional) Proporcionar esquema de configuración del complemento de EKS

Para la versión del complemento, si elige la v1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del agente de GuardDuty. Para obtener información sobre los rangos de parámetros, consulte [Configurar los parámetros del complemento de EKS](#).

- a. Amplíe Ajustes de configuración opcionales para ver los parámetros que se pueden configurar y su valor y formato previstos.
 - b. Establezca los parámetros. Los valores deben estar en el rango proporcionado en [Configurar los parámetros del complemento de EKS](#).
 - c. Elija Guardar cambios para crear el complemento según la configuración avanzada.
 - d. En Método de resolución de conflictos, la opción que elija se utilizará para resolver conflictos en caso de que actualice el valor de un parámetro a un valor que no sea el predeterminado. Para obtener más información sobre las opciones enumeradas, consulte [resolveConflicts](#) en la Referencia de la API de Amazon EKS.
10. Elija Siguiente.
 11. En la página Revisar y crear, compruebe todos los detalles y elija Crear.
 12. Vuelva a los detalles del clúster y elija la pestaña Recursos.
 13. Puede ver los nuevos pods con el prefijo aws-guardduty-agent.

API/CLI

Puede configurar el agente del complemento de Amazon EKS (aws-guardduty-agent) mediante una de las siguientes opciones:

- Ejecute [CreateAddon](#) para la cuenta.

-

Note

Para la versión del complemento, si elige la v1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del agente de GuardDuty. Para obtener más información, consulte [Configurar los parámetros del complemento de EKS](#).

Utilice los siguientes valores para los parámetros de la solicitud:

- En `addonName`, introduzca `aws-guardduty-agent`.

Puede utilizar el siguiente ejemplo de AWS CLI cuando utilice valores que se pueden configurar compatibles con las versiones v1.5.0 y posteriores del complemento. Asegúrese de sustituir los valores del marcador de posición resaltados en rojo y el `Example.json` asociado por los valores configurados.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.11.0-eksbuild.2 --configuration-values 'file://example.json'
```

Example `Example.json`

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

- Para obtener más información sobre los valores de `addonVersion` admitidos, consulte [Versiones de Kubernetes compatibles con el agente de seguridad de GuardDuty](#).
- Como alternativa también puede utilizar la AWS CLI. Para obtener más información, consulte [create-addon](#).

Nombres de DNS privados para el punto de conexión de VPC

De forma predeterminada, el agente de seguridad resuelve el nombre de DNS privado del punto de conexión de VPC y se conecta a este. En el caso de un punto de conexión que no sea FIPS, su DNS privado aparecerá en el siguiente formato:

Punto de conexión no FIPS: `guardduty-data.us-east-1.amazonaws.com`

La Región de AWS, `us-east-1`, cambiará según su región.

Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS

Si administra el agente de seguridad de GuardDuty manualmente, será responsable de actualizarlo para la cuenta. Para recibir notificaciones sobre nuevas versiones del agente, puede suscribirse a una fuente RSS en [Versiones del agente de seguridad de GuardDuty](#).

Puede actualizar el agente de seguridad a la versión más reciente para aprovechar la compatibilidad y las mejoras introducidas. Si la compatibilidad estándar de la versión actual del agente está a punto de finalizar, para continuar con el uso de Runtime Monitoring (o Runtime Monitoring de EKS), deberá actualizar a la versión siguiente disponible o la más reciente del agente.

Requisito previo

Antes de actualizar la versión del agente de seguridad, asegúrese de que la versión del agente que tiene previsto utilizar ahora sea compatible con la versión de Kubernetes. Para obtener más información, consulte [Versiones de Kubernetes compatibles con el agente de seguridad de GuardDuty](#).

Console

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. Elija un nombre para el clúster.
3. En la información del clúster, seleccione la pestaña Complementos.
4. En la pestaña Complementos, seleccione Runtime Monitoring de GuardDuty.
5. Elija Editar para actualizar los detalles del agente.
6. En la página Configurar Runtime Monitoring de GuardDuty, actualice los detalles.

7. (Opcional) Actualizar los valores de configuración opcionales

Si la versión del complemento de EKS es la 1.5.0 o una posterior, también puede actualizar el esquema de configuración del complemento.

- a. Amplíe los Ajustes de configuración opcionales para ver el esquema de configuración.
- b. Actualice los valores del parámetro en función del rango proporcionado en [Configurar los parámetros del complemento de EKS](#).
- c. Elija Guardar cambios para iniciar la actualización.
- d. En Método de resolución de conflictos, la opción que elija se utilizará para resolver conflictos en caso de que actualice el valor de un parámetro a un valor que no sea el predeterminado. Para obtener más información sobre las opciones enumeradas, consulte [resolveConflicts](#) en la Referencia de la API de Amazon EKS.

API/CLI

Para actualizar el agente de seguridad de GuardDuty para sus clústeres de Amazon EKS, consulte [Actualización de un complemento](#).

Note

Para la versión del complemento, si elige la 1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del agente de GuardDuty. Para obtener información sobre los rangos de parámetros, consulte [Configurar los parámetros del complemento de EKS](#).

Puede utilizar el siguiente ejemplo de AWS CLI cuando utilice valores que se pueden configurar compatibles con las versiones 1.5.0 y posteriores del complemento. Asegúrese de sustituir los valores del marcador de posición resaltados en rojo y el `Example.json` asociado por los valores configurados.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.11.0-eksbuild.2 --configuration-values 'file://example.json'
```

Example Example.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

Si la versión del complemento de Amazon EKS es 1.5.0 o posterior y ha configurado el esquema del complemento, puede comprobar si los valores aparecen correctamente para el clúster. Para obtener más información, consulte [Verificar las actualizaciones del esquema de configuración](#).

Configurar los parámetros del agente de seguridad de GuardDuty (complemento) para Amazon EKS

Puede configurar parámetros específicos del agente de seguridad de GuardDuty para Amazon EKS. Esta compatibilidad se encuentra disponible para la versión 1.5.0 y posteriores del agente de seguridad de GuardDuty. Para obtener información sobre las versiones más recientes del complemento, consulte [Versiones del agente de seguridad GuardDuty para los recursos de Amazon EKS](#).

Por qué debo actualizar el esquema de configuración del agente de seguridad

El esquema de configuración para el agente de seguridad de GuardDuty es el mismo en todos los contenedores dentro de los clústeres de Amazon EKS. Cuando los valores predeterminados no se ajusten a las cargas de trabajo asociadas ni al tamaño de la instancia, considere la posibilidad de configurar los ajustes de la CPU, memoria, PriorityClass y dnsPolicy. Independientemente de cómo administre el agente de GuardDuty para los clústeres de Amazon EKS, puede ajustar o actualizar la configuración existente de estos parámetros.

Comportamiento de configuración automatizada del agente con parámetros configurados

Cuando GuardDuty administra el agente de seguridad (complemento de EKS) en su nombre, actualiza el complemento, según sea necesario. GuardDuty establecerá el valor de los parámetros que se pueden configurar en un valor predeterminado. Sin embargo, es posible actualizar los parámetros al valor deseado. Si esto provoca un conflicto, la opción predeterminada para [resolveConflicts](#) es None.

Parámetros y valores que se pueden configurar

Para obtener información sobre los pasos a seguir para configurar los parámetros del complemento, consulte:

- [Instalar manualmente el agente de seguridad de GuardDuty en los recursos de Amazon EKS](#) o
- [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#)

En las siguientes tablas se indican los rangos y valores que puede utilizar para implementar el complemento de Amazon EKS manualmente o actualizar la configuración existente del complemento.

Configuración de la CPU

Parámetros	Valor predeterminado	Rango configurable
Solicitudes	200m	Entre 200m y 10000m, incluidos ambos
Límites	1000m	

Configuración de memoria

Parámetros	Valor predeterminado	Rango configurable
Solicitudes	256Mi	Entre 256Mi y 20000Mi, ambos incluidos
Límites	1024Mi	

PriorityClass Configuración de

Cuando GuardDuty crea un complemento de Amazon EKS en su nombre, el `PriorityClass` asignado es `aws-guardduty-agent.priorityclass`. Esto significa que no se tomará ninguna medida en función de la prioridad del pod del agente. Para configurar este parámetro del complemento, elija una de las siguientes opciones de `PriorityClass`:

PriorityClass configura	preemptio	Descripción de preemptio	Valor del pod
ble	nPolicy Valc	nPolicy	
	de		
<code>aws-guardduty-agent.priorityclass</code>	Never	Sin acciones	1000000
<code>aws-guardduty-agent.priorityclass-high</code>	PreemptLowerPriority	Asignar este valor dará prioridad a un pod en ejecución con un valor de prioridad inferior al valor del pod del agente.	100000000
<code>system-cluster-critical</code> ¹	PreemptLowerPriority		2000000000
<code>system-node-critical</code> ¹	PreemptLowerPriority		2000001000

¹ Kubernetes proporciona estas dos opciones de `PriorityClass`: `system-cluster-critical` y `system-node-critical`. Para obtener más información, consulte [PriorityClass](#) en la documentación de Kubernetes.

dnsPolicy Configuración de

Elija una de las siguientes opciones de política de DNS compatibles con Kubernetes. Cuando no se especifica ninguna configuración, `ClusterFirst` se utiliza como valor predeterminado.

- `ClusterFirst`
- `ClusterFirstWithHostNet`

- Default

Para obtener información sobre estas políticas, consulte [Política de DNS del pod](#) en la documentación de Kubernetes.

Verificar las actualizaciones del esquema de configuración

Una vez configurados los parámetros, siga los siguientes pasos para comprobar que el esquema de configuración se ha actualizado:

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la página Clústeres, seleccione el Nombre del clúster cuyas actualizaciones desea verificar.
4. Elija la pestaña Recursos.
5. En el panel Tipos de recursos, en Cargas de trabajo, elija DaemonSets.
6. Seleccione aws-guardduty-agent.
7. En la página aws-guardduty-agent, elija Vista sin procesar para ver la respuesta JSON sin formato. Compruebe que los parámetros que se pueden configurar muestran el valor proporcionado.

Después de verificar, cambie a la consola de GuardDuty. Seleccione la Región de AWS correspondiente y vea el estado de cobertura para los clústeres de Amazon EKS. Para obtener más información, consulte [Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS](#).

Validar la configuración del punto de conexión de VPC

Después de instalar el agente de seguridad manualmente o a través de la configuración automatizada de GuardDuty, puede utilizar este documento para validar la configuración del punto de conexión de VPC. También puede seguir estos pasos después de solucionar cualquier [problema de cobertura en tiempo de ejecución](#) para un tipo de recurso. Puede asegurarse de que los pasos han funcionado según lo previsto, y la cobertura podría aparecer en Buen estado.

Siga los siguientes pasos para validar que la configuración del punto de conexión de VPC para el tipo de recurso se ha establecido correctamente en la cuenta de propietario de VPC:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, en Nube privada virtual, seleccione Sus VPC.
3. En la página Sus VPC, elija el CIDR de IPv4 asociado a su ID de VPC.
4. En el panel de navegación, en Nube virtual privada, seleccione Puntos de conexión.
5. En la tabla Puntos de conexión, seleccione la fila cuyo Nombre de servicio sea similar a com.amazonaws.**us-east-1**.guardduty-data. La región (us-east-1) podría ser diferente para el punto de conexión.
6. Aparecerá un panel para los detalles del punto de conexión. En la pestaña Grupos de seguridad, seleccione el enlace correspondiente al ID del grupo asociado para obtener más detalles.
7. En la tabla de Grupos de seguridad, seleccione la fila con el ID del grupo de seguridad asociado para ver los detalles.
8. En la pestaña Reglas de entrada, asegúrese de que exista una política de ingreso con el Rango de puertos configurado como 443 y el Origen como el valor copiado desde el CIDR de IPv4. Las reglas de entrada controlan el tráfico entrante autorizado a alcanzar la instancia. La siguiente imagen muestra las reglas de entrada para un grupo de seguridad asociado a la VPC utilizada por el agente de seguridad de GuardDuty.

Si aún no tiene un grupo de seguridad que tenga habilitado un puerto de entrada 443, [Cree un grupo de seguridad](#) en la Guía del usuario de Amazon EC2.

Si se produce un problema al restringir los permisos de entrada a la VPC (o clúster), admita el puerto de entrada 443 desde cualquier dirección IP (0.0.0.0/0).

La siguiente lista incluye elementos que conviene conocer después de instalar o actualizar el agente de seguridad.

Evaluar la cobertura en tiempo de ejecución

El siguiente paso después de instalar o actualizar el agente de seguridad consiste en evaluar la cobertura en tiempo de ejecución de los recursos. Si la cobertura en tiempo de ejecución está en mal estado, debe solucionar el problema. Para obtener más información, consulte [Problemas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Si la cobertura en tiempo de ejecución está en buen estado, indica que la Supervisión en tiempo de ejecución puede recopilar y recibir eventos en tiempo de ejecución. Para obtener una lista de estos eventos, consulte [Tipos de eventos de tiempo de ejecución recopilados](#).

Nombre de DNS privado para puntos de conexión

Después de instalar el agente de seguridad de GuardDuty para los recursos, de forma predeterminada, resolverá el nombre de DNS privado del punto de conexión de VPC y se conectará a este. En el caso de un punto de conexión que no sea FIPS, el DNS privado aparecerá en el siguiente formato:

```
guardduty-data.us-east-1.amazonaws.com
```

La Región de AWS, *us-east-1*, cambiará según su región.

Un host se puede instalar con dos agentes de seguridad

Al utilizar el agente de seguridad de GuardDuty para una instancia de Amazon EC2, es posible instalar y utilizar el agente en el host subyacente dentro de un clúster de Amazon EKS. Si ya había implementado un agente de seguridad en ese clúster de EKS, pueden haber dos agentes de seguridad en ejecución en el mismo host al mismo tiempo. Para obtener información sobre cómo funciona GuardDuty en este escenario, consulte [Agentes de seguridad en el mismo host](#).

Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas

Después de habilitar la Supervisión en tiempo de ejecución y de la implementación del agente de seguridad de GuardDuty en el recurso, GuardDuty proporciona estadísticas de cobertura para el tipo de recurso correspondiente y el estado de cobertura individual para los recursos que pertenecen a la cuenta. Para determinar el estado de la cobertura, asegúrese de que ha habilitado la Supervisión en tiempo de ejecución, de que se ha creado el punto de conexión de Amazon VPC y de que se ha implementado el agente de seguridad de GuardDuty para el recurso correspondiente. Cuando la cobertura está en buen estado, significa que, si hay un evento en tiempo de ejecución relacionado con el recurso, GuardDuty podrá recibir dicho evento a través del punto de conexión de Amazon VPC y supervisar el comportamiento. Si se produjo un problema al configurar la Supervisión en tiempo de ejecución, al crear un punto de conexión de Amazon VPC o al implementar el agente de seguridad de GuardDuty, la cobertura aparecerá en mal estado. Si la cobertura está en mal estado, GuardDuty no podrá recibir ni supervisar el comportamiento en tiempo de ejecución del recurso correspondiente, así como tampoco podrá generar resultados de Supervisión en tiempo de ejecución.

Los siguientes temas resultan útiles a la hora de revisar las estadísticas de cobertura, configurar las notificaciones de EventBridge y solucionar los problemas de cobertura para un tipo de recurso específico.

Contenido

- [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#)
- [Cobertura y solución de problemas en tiempo de ejecución para clústeres de Amazon ECS](#)
- [Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS](#)

Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2

Para los recursos de Amazon EC2, la cobertura en tiempo de ejecución se evalúa a nivel de instancia. Las instancias de Amazon EC2 pueden ejecutar varios tipos de aplicaciones y cargas de trabajo, entre otros, en el entorno de AWS. Esta característica también admite las instancias de Amazon EC2 administradas por Amazon ECS y, si tiene clústeres de Amazon ECS que se ejecutan en una instancia de Amazon EC2, los problemas de cobertura a nivel de instancia aparecerán en la cobertura en tiempo de ejecución de Amazon EC2.

Temas

- [Revisión de las estadísticas de cobertura](#)
- [Cambio del estado de la cobertura con las notificaciones de EventBridge](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#)

Revisión de las estadísticas de cobertura

Las estadísticas de cobertura para las instancias de Amazon EC2 asociadas a cuentas propias o a cuentas de miembro corresponden al porcentaje de instancias de EC2 en buen estado respecto al total de instancias de EC2 de la Región de AWS seleccionada. La siguiente ecuación lo representa de la siguiente manera:

$$(\text{Instancias en buen estado} / \text{Todas las instancias}) * 100$$

Si también ha implementado el agente de seguridad de GuardDuty para los clústeres de Amazon ECS, cualquier problema de cobertura a nivel de instancia asociado a los clústeres de Amazon ECS que se ejecuten en una instancia de Amazon EC2 aparecerá como un problema de cobertura en tiempo de ejecución de la instancia de Amazon EC2.

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

Console

- Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
- En el panel de navegación, elija Supervisión en tiempo de ejecución.
- Elija la pestaña Cobertura en tiempo de ejecución.
- En la pestaña Cobertura en tiempo de ejecución de instancias de EC2, puede ver las estadísticas de cobertura agregadas por el estado de cobertura de cada instancia de Amazon EC2 que esté disponible en la tabla de la lista de instancias.
- Puede filtrar la tabla Lista de instancias por las siguientes columnas:
 - ID de cuenta
 - Tipo de administración del agente
 - Versión del agente
 - Estado de la cobertura
 - ID de instancia
 - ARN del clúster
- Si alguna de las instancias de EC2 tiene la cobertura en mal estado, la columna Problema incluye información adicional sobre el motivo del mal estado.

API/CLI

- Ejecute la API [ListCoverage](#) con el ID de detector válido propio, la región actual y el punto de conexión del servicio. Puede filtrar y ordenar la lista de instancias a través de esta API.
- Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
 - `ACCOUNT_ID`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `AGENT_VERSION`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
 - `CLUSTER_ARN`

- Cuando `filter-criteria` incluye `RESOURCE_TYPE` como EC2, la Supervisión en tiempo de ejecución no admite el uso de `PROBLEMA` como el `AttributeName`. Si lo utiliza, la respuesta de la API generará una `InvalidInputException`.

Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:

- `ACCOUNT_ID`
- `COVERAGE_STATUS`
- `INSTANCE_ID`
- `UPDATED_AT`
- Puede cambiar el valor de *max-results* (hasta 50).
- Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
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
```

- Ejecute la API [GetCoverageStatistics](#) para recuperar las estadísticas agregadas de cobertura según `statisticsType`.
- Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
 - `COUNT_BY_COVERAGE_STATUS`: representa las estadísticas de cobertura de los clústeres de EKS agregadas por estado de cobertura.
 - `COUNT_BY_RESOURCE_TYPE`: estadísticas de cobertura agregadas en función del tipo de recurso de AWS de la lista.
- Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
 - `ACCOUNT_ID`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `AGENT_VERSION`
 - `MANAGEMENT_TYPE`

- INSTANCE_ID
- CLUSTER_ARN
- Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si la cobertura de la instancia de EC2 está en mal estado, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#).

Cambio del estado de la cobertura con las notificaciones de EventBridge

Es posible que la cobertura de la instancia de Amazon EC2 aparezca en mal estado. Para mantenerse informado sobre los cambios en el estado de la cobertura, recomendamos supervisar periódicamente su estado y solucionar cualquier problema si esta se encuentra en mal estado. Como alternativa, puede crear una regla de Amazon EventBridge para recibir notificaciones cuando la cobertura cambie de estar en mal estado a buen estado, o viceversa. De forma predeterminada, GuardDuty publica esto en el [bus de EventBridge](#) de su cuenta.

Ejemplo de esquema de notificaciones

En una regla de EventBridge, puede usar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación de estado de cobertura. Para obtener más información sobre cómo crear una regla de EventBridge, consulte [Create rule](#) en la Guía del usuario de Amazon EventBridge.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de la cobertura de la instancia de Amazon EC2 cambie de Healthy a Unhealthy, el detail-type debe ser *Protección en tiempo de ejecución de GuardDuty en mal estado*. Para recibir una notificación cuando el estado de cobertura cambie de Unhealthy a Healthy, sustituya el valor de detail-type por *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de 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"
  }
}
```

Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2

Si la cobertura de la instancia de Amazon EC2 está en mal estado, puede ver el motivo en la columna Problema.

Si la instancia de EC2 está asociada a un clúster de EKS y el agente de seguridad para EKS se instaló manualmente o mediante la configuración automatizada del agente, para solucionar el problema de cobertura, consulte [Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS](#).

En la siguiente tabla se enumeran los tipos de problemas y los pasos de resolución de problemas correspondientes.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
No hay generación de informes de agentes	A la espera de la notificación SSM	Recibir la notificación SSM puede tardar unos minutos. Asegúrese de que SSM administra la instancia de Amazon EC2. Para obtener más información, consulte los pasos indicados en Método 1: mediante AWS Systems Manager en Instalación manual del agente de seguridad.
		Si administra el agente de seguridad de GuardDuty manualmente, asegúrese de haber seguido los pasos indicados en Administrar manualmente el agente de seguridad para el recurso de Amazon EC2.
	(Vacío a propósito)	Si ha habilitado la configuración automatizada del agente: • La instancia de EC2 es administrada por SSM. • Consulte periódicamente el estado del agente de seguridad. Para obtener más información, consulte Validar el estado de

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
		instalación del agente de seguridad de GuardDuty. Compruebe que el punto de conexión de VPC para la instancia de Amazon EC2 está configurado correctamente. Para obtener más información, consulte Validar la configuración del punto de conexión de VPC. Si la organización cuenta con una política de control de servicio (SCP), valide que el límite de permisos no restringe el permiso <code>guardduty:SendSecurityTelemetry</code>. Para obtener más información, consulte Validación de la política de control de servicios de la organización en un entorno de varias cuentas.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
	Agente desconectado	• Consulte el estado del agente de seguridad. Para obtener más información, consulte Validar el estado de instalación del agente de seguridad de GuardDuty. • Consulte los registros del agente de seguridad para identificar la posible causa raíz. Los registros proporcionan errores detallados que puede utilizar para solucionar el problema por su cuenta. Los archivos de registro están disponibles en <code>/var/log/amzn-guardduty-agent/</code>. Realice <code>sudo journalctl -u amazon-guardduty-agent</code>.
Agente no aprovisionado	Las instancias con etiquetas de exclusión se excluyen de Runtime Monitoring.	GuardDuty no recibe eventos de tiempo de ejecución de las instancias de Amazon EC2 que se lanzan con la etiqueta de exclusión <code>GuardDutyManaged :false</code>. Para recibir eventos de tiempo de ejecución de esta instancia de Amazon EC2, elimine la etiqueta de exclusión.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
	La versión del kernel es inferior a la versión compatible.	Para obtener información sobre las versiones de kernel compatibles en todas las distribuciones de sistemas operativos, consulte Validar los requisitos de arquitectura para las instancias de Amazon EC2.
	La versión del kernel es superior a la versión compatible.	Para obtener información sobre las versiones de kernel compatibles en todas las distribuciones de sistemas operativos, consulte Validar los requisitos de arquitectura para las instancias de Amazon EC2.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
	No se puede recuperar el documento de identidad de la instancia	Siga estos pasos: 1. Confirme que su recurso sea una instancia de Amazon EC2 y no una instancia híbrida que no sea EC2. 2. Confirme que el servicio de metadatos de instancia s (IMDS) esté habilitado. Para hacerlo, consulte Configuración de las opciones del servicio de metadatos de instancias en la Guía del usuario de Amazon EC2. 3. Verifique que el documento de identidad de la instancia existe. Para ello, consulte Recuperar el documento de identidad de la instancia en la Guía del usuario de Amazon EC2. 4. Si el documento de identidad de la instancia sigue sin existir, reinicie la instancia. El documento de identidad de la instancia se genera cuando la instancia se detiene e inicia, se reinicia o se inicia.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
Se produjo un error al crear la asociación de SSM	La asociación de SSM con GuardDuty ya existe en la cuenta	1. Elimine manualmente la asociación existente. Para obtener más información, consulte Eliminar asociaciones en la Guía del usuario de AWS Systems Manager. 2. Después de eliminar la asociación, desactive y vuelva a habilitar la configuración automatizada del agente de GuardDuty para Amazon EC2.
	La cuenta tiene demasiadas asociaciones SSM	Seleccione una de las siguientes dos opciones: • Elimine cualquier asociación de SSM que no se utilice. Para obtener más información, consulte Eliminar asociaciones en la Guía del usuario de AWS Systems Manager. • Verifique si la cuenta cumple los requisitos para un aumento de cuota. Para obtener más información, consulte Service Quotas de Systems Manager en Referencia general de AWS.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
Se produjo un error en la actualización de la asociación de SSM	La asociación de SSM con GuardDuty no existe en la cuenta	La asociación de SSM con GuardDuty no está presente en la cuenta. Desactive y vuelva a habilitar la supervisión en tiempo de ejecución.
Se produjo un error al eliminar la asociación de SSM	La asociación de SSM con GuardDuty no existe en la cuenta	La asociación de SSM con GuardDuty no está presente en la cuenta. Si la asociación de SSM se eliminó intencionalmente, no es necesario realizar ninguna acción.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
Se produjo un error en la ejecución de la asociación de la instancia de SSM	No se cumplen los requisitos de arquitectura u otros requisitos previos.	Para obtener información sobre distribuciones de sistemas operativos verificadas, consulte Requisitos previos para la compatibilidad con instancias de Amazon EC2. Si el problema persiste, los siguientes pasos le ayudarán a identificarlo y posiblemente a resolverlo: 1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/. 2. En el panel de navegación, en Administración de nodos, seleccione Administrador de estados. 3. Filtre por la propiedad Nombre del documento e ingrese AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Seleccione el ID de asociación correspondiente y consulte su Historial de ejecución.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
		5. Utilice el historial de ejecución para ver los errores, identificar la posible causa raíz e intentar resolverla.
Se produjo un error al crear el punto de conexión de VPC	No se admite la creación de puntos de conexión de VPC para la VPC compartida <i>vpcId</i>	La Supervisión en tiempo de ejecución admite el uso de una VPC compartida dentro de una organización. Para obtener más información, consulte Uso de VPC compartida con Runtime Monitoring.
	Solo cuando se utiliza una VPC compartida con una configuración automatizada del agente El ID de cuenta del propietario <i>111122223333</i> correspondiente a la VPC compartida <i>vpcId</i> no tiene habilitada la Supervisión en tiempo de ejecución, la configuración automatizada del agente, o ambas.	La cuenta de propietario de la VPC compartida debe habilitar la Supervisión en tiempo de ejecución y la configuración automatizada del agente para al menos un tipo de recurso (Amazon EKS o Amazon ECS [AWS Fargate]). Para obtener más información, consulte Requisitos previos específicos de la Supervisión en tiempo de ejecución de GuardDuty.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
	La habilitación del DNS privado requiere que los atributos de VPC <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> estén establecidos en <code>true</code> para <i>vpcId</i> (Servicio: Ec2, Código de estado: 400, ID de solicitud: <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>).	Asegúrese de que los siguientes atributos de VPC estén establecidos en <code>true</code> - <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> . Para obtener más información, consulte Atributos DNS para la VPC. Si utiliza la consola de Amazon VPC en https://console.aws.amazon.com/vpc/ para crear la VPC de Amazon, seleccione Habilitar nombres de host DNS y Habilitar la resolución de DNS. Para obtener más información, consulte Opciones de configuración de la VPC. Tras actualizar los atributos de la VPC, debe acelerar el reintento de creación del punto de conexión de la VPC al realizar uno de estos cambios: • Puede añadir o modificar la etiqueta <code>GuardDutyManaged</code> de su instancia de Amazon EC2 (recomendado). Por ejemplo, puede añadir <code>GuardDutyManaged</code> :<code>true</code> para

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
		incluir la instancia dRuntime Monitoring. • Puede cambiar el estado de la instancia Amazon EC2 (detener o reiniciar).

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
Se produjo un error al eliminar el punto de conexión de la VPC compartida	No se permite eliminar el punto de conexión de VPC compartida para el ID de cuenta 111122223333 , la VPC compartida vpcId , el ID de cuenta de propietario 555555555555 .	Medidas posibles: • Al desactivar el estado de la Supervisión en tiempo de ejecución de la cuenta de participante de la VPC compartida, no se afecta a la política de punto de conexión de VPC compartida ni al grupo de seguridad que existe en la cuenta de propietario. Para eliminar el punto de conexión de VPC compartida y el grupo de seguridad, debe desactivar la Supervisión en tiempo de ejecución o el estado de la configuración automatizada del agente en la cuenta de propietario de la VPC compartida. • La cuenta participante de la VPC compartida no puede eliminar el punto de conexión de la VPC compartida ni el grupo de seguridad alojados en la cuenta propietaria de la VPC compartida.

Tipo de problema	Mensaje del problema	Pasos para la solución de problemas
El agente no genera informes	(Vacío a propósito)	El tipo de problema ya no tiene soporte. Si el problema persiste y aún no ha habilitado o el agente automatizado de GuardDuty para Amazon EC2, hágalo. Si el problema persiste, considere la posibilidad de desactivar la Supervisión en tiempo de ejecución durante unos minutos y, a continuación, vuelva a habilitarla.

Cobertura y solución de problemas en tiempo de ejecución para clústeres de Amazon ECS

La cobertura en tiempo de ejecución para los clústeres de Amazon ECS incluye las tareas que se ejecutan en AWS Fargate y las instancias de contenedor ¹ de Amazon ECS.

Si se trata de un clúster de Amazon ECS que se ejecuta en Fargate, la cobertura en tiempo de ejecución se evalúa a nivel de tarea. La cobertura en tiempo de ejecución de los clústeres de ECS incluye las tareas de Fargate que se han comenzado a ejecutar después de habilitar la Supervisión en tiempo de ejecución y la configuración automatizada del agente para Fargate (solo ECS). Las tareas de Fargate son inmutables de forma predeterminada. GuardDuty no podrá instalar el agente de seguridad para supervisar contenedores en tareas ya en ejecución. Para incluir una tarea de Fargate de este tipo, debe detener e iniciar de nuevo la tarea. Asegúrese de verificar si el servicio asociado es compatible.

Para obtener información sobre el contenedor de Amazon ECS, consulte [Creación de capacidad](#).

Contenido

- [Revisión de las estadísticas de cobertura](#)
- [Cambio del estado de la cobertura con las notificaciones de EventBridge](#)

- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon ECS-Fargate](#)

Revisión de las estadísticas de cobertura

Las estadísticas de cobertura correspondientes a los recursos de Amazon ECS asociados a la cuenta propia o a las cuentas de miembro representan el porcentaje de los clústeres de Amazon ECS en buen estado sobre todos los clústeres de Amazon ECS en la Región de AWS seleccionada. Esto incluye la cobertura para clústeres de Amazon ECS asociados tanto a instancias de Fargate como de Amazon EC2. La siguiente ecuación lo representa de la siguiente manera:

$(\text{Clústeres en buen estado} / \text{Todos los clústeres}) * 100$

Consideraciones

- Las estadísticas de cobertura correspondientes al clúster de ECS incluyen el estado de cobertura de las tareas de Fargate o las instancias de contenedor de ECS asociadas a ese clúster de ECS. El estado de cobertura de las tareas de Fargate incluye tareas que están en estado de ejecución o que han terminado de ejecutarse recientemente.
- En la pestaña Cobertura en tiempo de ejecución de clústeres de ECS, el campo Instancias de contenedor cubiertas indica el estado de cobertura de las instancias de contenedor asociadas al clúster de Amazon ECS.

Si el clúster de Amazon ECS solo contiene tareas de Fargate, el recuento aparece como 0/0.

- Si el clúster de Amazon ECS está asociado a una instancia de Amazon EC2 que no cuenta con un agente de seguridad, la cobertura del clúster de Amazon ECS también estará en mal estado.

Para identificar y solucionar el problema de cobertura correspondiente a la instancia de Amazon EC2 asociada, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#) para instancias de Amazon EC2.

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

Console

- Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
- En el panel de navegación, elija Supervisión en tiempo de ejecución.
- Elija la pestaña Cobertura en tiempo de ejecución.

- En la pestaña Cobertura en tiempo de ejecución de clústeres de ECS, puede ver las estadísticas de cobertura agregadas por el estado de cobertura de cada clúster de Amazon ECS que esté disponible en la tabla Lista de clústeres.
- Puede filtrar la tabla Lista de clústeres por las siguientes columnas:
 - Identificador* de cuenta
 - Nombre del clúster
 - Tipo de administración del agente
 - Estado de la cobertura
- Si la cobertura de alguno de los clústeres de Amazon ECS está en mal estado, la columna Problema incluye información adicional sobre el motivo del mal estado.

Si los clústeres de Amazon ECS están asociados a una instancia de Amazon EC2, vaya a la pestaña Cobertura en tiempo de ejecución de la instancia de EC2 y filtre por el campo Nombre del clúster para ver el problema asociado.

API/CLI

- Ejecute la API [ListCoverage](#) con el ID de detector válido propio, la región actual y el punto de conexión del servicio. Puede filtrar y ordenar la lista de instancias a través de esta API.
- Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`
- Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:
 - `ACCOUNT_ID`
 - `COVERAGE_STATUS`
 - `ISSUE`
 - `ECS_CLUSTER_NAME`
 - `UPDATED_AT`

El campo se actualiza únicamente cuando se crea una nueva tarea en el clúster de Amazon ECS asociado o se produce un cambio en el estado de cobertura correspondiente.

- Puede cambiar el valor de *max-results* (hasta 50).
- Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
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
```

- Ejecute la API [GetCoverageStatistics](#) para recuperar las estadísticas agregadas de cobertura según `statisticsType`.
- Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
 - `COUNT_BY_COVERAGE_STATUS`: representa las estadísticas de cobertura de los clústeres de ECS agregadas por estado de cobertura.
 - `COUNT_BY_RESOURCE_TYPE`: estadísticas de cobertura agregadas en función del tipo de recurso de AWS de la lista.
- Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
- Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
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"}}] }'
```

Para obtener más información sobre los problemas de cobertura, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon ECS-Fargate](#).

Cambio del estado de la cobertura con las notificaciones de EventBridge

Es posible que el estado de cobertura del clúster de Amazon ECS aparezca como En mal estado. Para mantenerse informado sobre los cambios en el estado de la cobertura, recomendamos supervisar periódicamente su estado y solucionar cualquier problema si esta se encuentra en mal estado. Como alternativa, puede crear una regla de Amazon EventBridge para recibir notificaciones cuando la cobertura cambie de estar en mal estado a buen estado, o viceversa. De forma predeterminada, GuardDuty publica esto en el [bus de EventBridge](#) de su cuenta.

Ejemplo de esquema de notificaciones

En una regla de EventBridge, puede usar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación de estado de cobertura. Para obtener más información sobre cómo crear una regla de EventBridge, consulte [Create rule](#) en la Guía del usuario de Amazon EventBridge.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir notificaciones cuando el estado de cobertura del clúster de Amazon ECS cambie de Healthy a Unhealthy, el detail-type debe ser *Protección en tiempo de ejecución de GuardDuty en mal estado*. Para recibir una notificación cuando el estado de cobertura cambie de Unhealthy a Healthy, sustituya el valor de detail-type por *GuardDuty Runtime Protection Healthy*.

```
{  
  "version": "0",  
  "id": "event ID",  
  "detail-type": "GuardDuty Runtime Protection Unhealthy",  
  "source": "aws.guardduty",  
  "account": "Cuenta de AWS ID",  
  "time": "event timestamp (string)",  
  "region": "Región de 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"
  }
}

```

Resolución de problemas de cobertura en tiempo de ejecución de Amazon ECS-Fargate

Si la cobertura del clúster de Amazon ECS está en mal estado, puede ver el motivo en la columna Problema.

En la siguiente tabla se indican los pasos recomendados para solucionar los problemas relacionados con Fargate (solo Amazon ECS). Para obtener información sobre problemas de cobertura de instancias de Amazon EC2, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#) para instancias de Amazon EC2.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
El agente no genera informes	El agente no genera informes para las tareas en TaskDefin	Valide que el punto de conexión de VPC para la tarea del clúster de Amazon ECS

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	<pre>ition - ' <i>TASK_DEFINITION</i> '</pre>	esté configurado correctamente. Para obtener más información, consulte Validar la configuración del punto de conexión de VPC. Si la organización cuenta con una política de control de servicio (SCP), valide que el límite de permisos no restringe el permiso <code>guardduty:SendSecurityTelemetry</code>. Para obtener más información, consulte Validación de la política de control de servicios de la organización en un entorno de varias cuentas.
	<pre><i>VPC_ISSUE</i> ; for task in TaskDefinition - ' <i>TASK_DEFINITION</i> '</pre>	Consulte los detalles del problema de la VPC en la información adicional.
El agente salió	<pre>ExitCode: EXIT_CODE para tareas en TaskDefinition - ' <i>TASK_DEFINITION</i> '</pre>	Consulte los detalles del problema en la información adicional.
	<pre>Motivo: <i>REASON</i> para las tareas en TaskDefinition - ' <i>TASK_DEFINITION</i> '</pre>	

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	ExitCode: EXIT_CODE con el motivo: ' <i>EXIT_CODE</i> ' para las tareas en TaskDefinition - ' <i>TASK_DEFINITION</i> '	

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	El agente salió: Motivo: <code>CannotPullContainerError</code> : se ha vuelto a intentar extraer el manifiesto de imagen...	En este escenario, es posible que GuardDuty no pueda obtener la imagen del contenedor de sidecar. La tarea seguirá ejecutándose, pero GuardDuty no podrá detectar posibles amenazas. Realice los siguientes pasos de solución de problemas uno por uno para comprobar si esto ayuda a resolver el problema de cobertura: • Permisos: asegúrese de que su rol de ejecución de tareas tenga los permisos de ECR necesarios que se indican en Requisitos de los permisos. • Conectividad de red: verifique que sus tareas de Fargate puedan llegar al ECR a través del acceso público a Internet o de puntos de conexión de VPC configurados correctamente, como se describe en Requisitos de conectividad de red. • Configuración del grupo de seguridad: verifique que su grupo de seguridad permite el acceso saliente a la lista

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
		de prefijos gestionados de S3 en el puerto 443, como se explica en Configuración del grupo de seguridad. • Ejecute el manual de procedimientos de AWS Support-TroubleshootECSTaskFailedToStart en la región de su clúster para identificar problemas específicos. • Consulte los registros de tareas para ver si hay mensajes de error. Para obtener más información sobre cómo hacerlo, consulte Ver registros del agente de contenedores de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service. Para obtener información sobre errores comunes y solución de problemas, consulte Solución de problemas de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
		Estos tres componentes (permisos, conectividad de red y configuración del grupo de seguridad) son independientes, pero todos son necesarios para descargar de manera correcta la imagen del contenedor de GuardDuty de Amazon ECR. Si el problema persiste, consulte Se producen errores inesperados en mi flujo de trabajo de AWS Step Functions.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
Se produjo un error al crear el punto de conexión de VPC	La habilitación del DNS privado requiere que los atributos de VPC <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> estén establecidos en <code>true</code> para <i>vpcId</i> (Servicio: EC2, Código de estado: 400, ID de solicitud: <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>).	Asegúrese de que los siguientes atributos de VPC estén establecidos en <code>true</code> - <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> . Para obtener más información, consulte Atributos DNS para la VPC. Si utiliza la consola de Amazon VPC en https://console.aws.amazon.com/vpc/ para crear la VPC de Amazon, asegúrese de seleccionar Habilitar nombres de host DNS y Habilitar la resolución de DNS. Para obtener más información, consulte Opciones de configuración de la VPC.
Agente no provisionado	Invocación no admitida por parte del <i>SERVICE</i> para tareas en TaskDefinition - <i>'TASK_DEFINITION'</i>	Esta tarea fue invocada por un <i>SERVICE</i> que no se admite.
	Arquitectura de CPU no admitida <i>"TYPE"</i> para tareas en TaskDefinition - <i>'TASK_DEFINITION'</i>	Esta tarea se ejecuta en una arquitectura de CPU no admitida. Para obtener información acerca de las arquitecturas de CPU compatibles, consulte Validación de los requisitos de arquitectura .

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	TaskExecutionRole falta en TaskDefinition - <code>'TASK_DEFINITION'</code>	Falta el rol de ejecución de tareas de ECS. Para obtener información sobre cómo proporcionar el rol de ejecución de tareas y los permisos necesarios, consulte Requisitos previos para el acceso a imágenes de contenedores.
	Falta la configuración de red <code>"CONFIGURATION_DETAILS"</code> para las tareas en TaskDefinition - <code>'TASK_DEFINITION'</code>	Los problemas de configuración de red pueden surgir debido a la falta de configuración de la VPC, o a la falta de subredes o subredes vacías. Compruebe que la configuración de la red es correcta. Para obtener más información, consulte Requisitos previos para el acceso a imágenes de contenedores. Para obtener más información, consulte Parámetros de definición de tareas de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	Las tareas iniciadas cuando los clústeres tenían una etiqueta de exclusión se excluyen de Runtime Monitoring. ID de tarea afectada (s): 'TASK_ID'	Al cambiar la etiqueta predefinida de GuardDuty de <code>GuardDutyManaged -true</code> a <code>GuardDutyManaged -false</code>, GuardDuty no recibirá los eventos en tiempo de ejecución para el clúster de Amazon ECS. Actualice la etiqueta a <code>GuardDutyManaged -true</code> y, a continuación, vuelva a iniciar la tarea.
	Los tareas implementadas cuando los clústeres tenían una etiqueta de exclusión se excluyen de Runtime Monitoring. Nombre(s) de los servicios afectados: 'SERVICE_NAME'	Cuando los servicios se implementen con la etiqueta de exclusión <code>GuardDutyManaged -false</code>, GuardDuty no recibirá eventos de tiempo de ejecución para este clúster de Amazon ECS. Actualice la etiqueta a <code>GuardDutyManaged -true</code> y, a continuación, vuelva a implementar el servicio.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	No se incluyen las tareas iniciadas antes de habilitar la configuración automática del agente. ID(s) de tarea afectada: ' TASK_ID '	Si el clúster contiene una tarea que se lanzó antes de habilitar la configuración del agente automatizado para Amazon ECS, GuardDuty no podrá protegerla. Vuelva a lanzar la tarea para que GuardDuty la monitoree.
	No se incluyen los servicios implementados antes de habilitar la configuración automática del agente. Nombre(s) de los servicios afectados: ' SERVICE_NAME '	Cuando los servicios se implementen antes de habilitar la configuración automática de agentes para Amazon ECS, GuardDuty no recibirá eventos de tiempo de ejecución para los clústeres de ECS.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
	El servicio ' <i>SERVICE_NAME</i> ' requiere una nueva implementación para corregir o solucionar problemas. Consulte la documentación y los nombres de los servicios afectados: ' <i>SERVICE_NAME</i> '	No se admite un servicio que se inició antes de habilitar Runtime Monitoring. Puede reiniciar el servicio o actualizarlo con la opción <code>forceNewDeployment</code> según los pasos que se indican en Actualización de un servicio de Amazon ECS mediante la consola en la Guía para desarrolladores de Amazon Elastic Container Service. Como alternativa, también puede seguir los pasos de UpdateService en la Referencia de la API de Amazon Elastic Container Service.
	Las tareas iniciadas antes de habilitar Runtime Monitoring requieren un relanzamiento. ID(s) de tarea afectada: ' <i>TASK_ID_1</i> '	Las tareas son inmutables en Amazon ECS. Para evaluar el comportamiento en tiempo de ejecución o una tarea de AWS Fargate en ejecución, asegúrese de que Runtime Monitoring ya está habilitada y, a continuación, reinicie la tarea para que GuardDuty agregue el sidecar de contenedor.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
Otros	Problema no identificado, para tareas en TaskDefinition - 'TASK_DEFINITION'	Utilice las siguientes preguntas para identificar la causa raíz del problema: • ¿La tarea se inició antes de habilitar la Supervisión en tiempo de ejecución? Las tareas son inmutables en Amazon ECS. Para evaluar el comportamiento en tiempo de ejecución de una tarea de Fargate en ejecución, asegúrese de que la Supervisión en tiempo de ejecución ya está habilitada y, a continuación, reinicie la tarea para que GuardDuty agregue el sidecar de contenedor. • ¿Esta tarea forma parte de una implementación de servicios que se inició antes de habilitar la Supervisión en tiempo de ejecución? En tal caso, puede reiniciar el servicio o actualizarlo con <code>forceNewDeployment</code>. Para ello, siga los pasos indicados en Actualizar un servicio. También puede utilizar UpdateService o AWS CLI.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
		• ¿La tarea se lanzó después de excluir el clúster de ECS de la Supervisión en tiempo de ejecución? Al cambiar la etiqueta predefinida de GuardDuty de GuardDuty Managed -true a GuardDuty Managed -false, GuardDuty no recibirá los eventos en tiempo de ejecución para el clúster de ECS. • ¿El servicio contiene una tarea que tiene un formato antiguo de taskArn? La Supervisión en tiempo de ejecución de GuardDuty no permite la cobertura para tareas que tienen el formato antiguo de taskArn. Para obtener información sobre los nombres de recursos de Amazon (ARN) para los recursos de Amazon ECS, consulte Nombres de recursos de Amazon (ARN) e ID.

Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS

Después de habilitar la Supervisión en tiempo de ejecución e instalar el agente de seguridad de GuardDuty (complemento) para EKS, ya sea manualmente o a través de la configuración automatizada del agente, podrá comenzar a evaluar la cobertura de los clústeres de EKS.

Contenido

- [Revisión de las estadísticas de cobertura](#)
- [Cambio del estado de la cobertura con las notificaciones de EventBridge](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS](#)

Revisión de las estadísticas de cobertura

Las estadísticas de cobertura de los clústeres de EKS asociados a sus propias cuentas o a las de sus miembros representan el porcentaje de los clústeres de EKS en buen estado con respecto a todos los clústeres de EKS de la Región de AWS seleccionada. La siguiente ecuación lo representa de la siguiente manera:

$$(\text{Clústeres en buen estado} / \text{Todos los clústeres}) * 100$$

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

Console

- Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
- En el panel de navegación, elija Supervisión en tiempo de ejecución.
- Seleccione la pestaña Cobertura del tiempo de ejecución de los clústeres de EKS.
- En la pestaña Cobertura del tiempo de ejecución de los clústeres de EKS, puede ver las estadísticas de cobertura agregadas por el estado de cobertura que está disponible en la tabla Lista de clústeres.
 - Puede filtrar la tabla Lista de clústeres por las siguientes columnas:
 - Nombre del clúster
 - ID de cuenta
 - Tipo de administración del agente

- Estado de la cobertura
- Versión del complemento
- Si el valor de Estado de la cobertura de alguno de sus clústeres de EKS es En mal estado, en la columna Problema se puede incluir información adicional sobre el motivo del estado En mal estado.

API/CLI

- Ejecute la API [ListCoverage](#) con sus propios ID de detector, región y punto de conexión de servicio válidos. Puede filtrar y ordenar la lista de clústeres con esta API.
- Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
 - ACCOUNT_ID
 - CLUSTER_NAME
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - ADDON_VERSION
 - MANAGEMENT_TYPE
- Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:
 - ACCOUNT_ID
 - CLUSTER_NAME
 - COVERAGE_STATUS
 - ISSUE
 - ADDON_VERSION
 - UPDATED_AT
- Puede cambiar el valor de `max-results` (hasta 50).
- Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty --region us-east-1 list-coverage --detector-
```

```
Id 12abc34d567e87a901bc2d34e56789f0 --sort-criteria '{"AttributeName":
```



```
"EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
'{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}]}] }' --max-results 5
```

- Ejecute la API [GetCoverageStatistics](#) para recuperar las estadísticas agregadas de cobertura según `statisticsType`.
- Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
 - `COUNT_BY_COVERAGE_STATUS`: representa las estadísticas de cobertura de los clústeres de EKS agregadas por estado de cobertura.
 - `COUNT_BY_RESOURCE_TYPE`: estadísticas de cobertura agregadas en función del tipo de recurso de AWS de la lista.
- Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `ADDON_VERSION`
 - `MANAGEMENT_TYPE`
- Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
"FilterCondition":{"EqualsValue":"123456789012"}]}] }'
```

Si el estado de cobertura de su clúster de EKS es En mal estado, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS](#).

Cambio del estado de la cobertura con las notificaciones de EventBridge

El estado de cobertura de un clúster de EKS de su cuenta puede aparecer como En mal estado. Para detectar cuándo el estado de cobertura pasa a ser En mal estado, le recomendamos que supervise el estado de cobertura periódicamente y que solucione los problemas si el estado es

En mal estado. Como alternativa, puede crear una regla de Amazon EventBridge para que se le notifique cuando el estado de cobertura cambie de Unhealthy a Healthy o viceversa. De forma predeterminada, GuardDuty publica esto en el [bus de EventBridge](#) de su cuenta.

Ejemplo de esquema de notificaciones

En una regla de EventBridge, puede usar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación de estado de cobertura. Para obtener más información sobre cómo crear una regla de EventBridge, consulte [Create rule](#) en la Guía del usuario de Amazon EventBridge.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir notificaciones cuando el estado de cobertura del clúster de Amazon EKS cambie de Healthy a Unhealthy, el detail-type debe ser *Protección en tiempo de ejecución de GuardDuty en mal estado*. Para recibir una notificación cuando el estado de cobertura cambie de Unhealthy a Healthy, sustituya el valor de detail-type por *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de 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"
  }
}

```

Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS

Si el estado de cobertura de su clúster de EKS es `Unhealthy`, puede ver el error correspondiente en la columna Problema de la consola de GuardDuty o mediante el tipo de datos [CoverageResource](#).

Cuando trabaje con etiquetas de inclusión o exclusión para supervisar los clústeres de EKS de forma selectiva, es posible que las etiquetas tarden algún tiempo en sincronizarse. Esto puede afectar al estado de cobertura del clúster de EKS asociado. Puede intentar eliminar y volver a agregar la etiqueta correspondiente (inclusión o exclusión). Para obtener más información, consulte [Etiquetado de los recursos de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

La estructura de un problema de cobertura es `Issue type:Extra information`. Por lo general, los problemas tienen información adicional opcional que puede incluir una excepción específica del cliente o una descripción del problema. Con base en la Información adicional, las siguientes tablas indican los pasos recomendados para solucionar los problemas de cobertura de los clústeres de EKS.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Se produjo un error al crear el complemento	El complemento <code>aws-guardduty-agent</code> no es compatible con la versión actual del clúster <code>ClusterName</code> . No se admite el complemento especificado.	Asegúrese de utilizar una de esas versiones de Kubernetes que admiten la implementación del complemento de EKS <code>aws-guardduty-agent</code> . Para obtener más información, consulte Versiones de Kubernetes compatibles con el agente de seguridad de GuardDuty . Para obtener información sobre cómo actualizar su versión

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
		de Kubernetes, consulte Actualización de una versión de Kubernetes de clúster de Amazon EKS .
Se produjo un error al crear el complemento Se produjo un error al actualizar el complemento El complemento está en mal estado	Problema con el complemento de EKS: AddonIssueCode : AddonIssueMessage	Para obtener información sobre los pasos recomendados para un código de problema de complemento específico, consulte Troubleshooting steps for Addon creation/updatation error with Addon issue code. Para obtener una lista de los códigos de problemas de complementos que se pueden encontrar en este problema, consulte AddonIssue.
Se produjo un error al crear el punto de conexión de VPC	No se admite la creación de puntos de conexión de VPC para la VPC compartida <i>vpcId</i>	La Supervisión en tiempo de ejecución ahora admite el uso de una VPC compartida dentro de una organización. Asegúrese de que las cuentas cumplen todos los requisitos previos. Para obtener más información, consulte Requisitos previos para utilizar una VPC compartida.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
	Solo cuando se utiliza una VPC compartida con una configuración automatizada del agente El ID de cuenta del propietario 111122223333 corresponde a la VPC compartida vpcId no tiene habilitada la Supervisión en tiempo de ejecución, la configuración automatizada del agente, o ambas. La habilitación del DNS privado requiere que los atributos de VPC <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> estén establecidos en <code>true</code> para vpcId (Servicio: Ec2, Código de estado: 400, ID de solicitud: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111).	La cuenta de propietario de la VPC compartida debe habilitar la Supervisión en tiempo de ejecución y la configuración automatizada del agente para al menos un tipo de recurso (Amazon EKS o Amazon ECS [AWS Fargate]). Para obtener más información, consulte Requisitos previos específicos de la Supervisión en tiempo de ejecución de GuardDuty. Asegúrese de que los siguientes atributos de VPC estén establecidos en <code>true</code> - <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> . Para obtener más información, consulte Atributos DNS para la VPC. Si utiliza la consola de Amazon VPC en https://console.aws.amazon.com/vpc/ para crear la VPC de Amazon, asegúrese de seleccionar Habilitar nombres de host DNS y Habilitar la resolución de DNS. Para obtener más información, consulte Opciones de configuración de la VPC.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Se produjo un error al eliminar el punto de conexión de la VPC compartida	No se permite eliminar el punto de conexión de VPC compartida para el ID de cuenta 111122223333 , la VPC compartida vpcId , el ID de cuenta de propietario 555555555555 .	Medidas posibles: - Al desactivar el estado de la Supervisión en tiempo de ejecución de la cuenta de participante de la VPC compartida, no se afecta a la política de punto de conexión de VPC compartida ni al grupo de seguridad que existe en la cuenta de propietario. Para eliminar el punto de conexión de VPC compartida y el grupo de seguridad, debe desactivar la Supervisión en tiempo de ejecución o el estado de la configuración automatizada del agente en la cuenta de propietario de la VPC compartida. - La cuenta participante de la VPC compartida no puede eliminar el punto de conexión de la VPC compartida ni el grupo de seguridad alojados en la cuenta propietaria de la VPC compartida.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Clústeres de EKS locales	Los complementos de EKS no se admiten en los clústeres de Outposts locales.	No se puede procesar. Para obtener más información, consulte Amazon EKS en AWS Outposts.
No se ha concedido el permiso de habilitación de la supervisión en tiempo de ejecución de EKS	(puede o no mostrar información adicional)	1. Si hay información adicional disponible sobre este problema, corrija la causa raíz y avance al siguiente paso. 2. Desactive la supervisión en tiempo de ejecución de EKS y vuelva a activarla. Asegúrese de que el agente de GuardDuty también se implementa, ya sea automáticamente a través de GuardDuty o manualmente.
Aprovisionamiento de recursos de habilitación de la supervisión en tiempo de ejecución de EKS en curso.	(puede o no mostrar información adicional)	No se puede procesar. Después de habilitar la supervisión en tiempo de ejecución de EKS, el estado de cobertura puede seguir siendo <code>Unhealthy</code> hasta que se complete el paso de aprovisionamiento de recursos. El estado de cobertura se supervisa y actualiza periódicamente.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Otros (cualquier otro problema)	Error debido a una falla de autorización	Desactive la supervisión en tiempo de ejecución de EKS y vuelva a activarla. Asegúrese de que el agente de GuardDuty también se implementa, ya sea automáticamente a través de GuardDuty o manualmente.

Pasos para solucionar un error de creación/actualización de un complemento con el código de error del complemento

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento EKS <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque no tiene la cantidad deseada de réplicas.	- Con el mensaje del problema, puede identificar y solucionar la causa raíz. Puede comenzar por describir el clúster. Por ejemplo, utilice kubectl describe pods para identificar la causa raíz del fallo de un pod. Después de solucionar la causa raíz, vuelva a intentar el paso (creación o actualización del complemento). - Si el problema persiste, compruebe que el punto de conexión de VPC para el clúster de Amazon EKS está configurado correctamente. Para obtener más información, consulte Validar la configuración del punto de conexión de VPC.

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods no están programados. Hay 0/x nodos disponibles: <code>x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never</code> .	Para resolver este problema, puede seguir uno de estos pasos: • Actualice la prioridad del pod del agente de GuardDuty: Parámetros y valores que se pueden configurar al configurar la <code>PriorityClass</code> para cualquiera de las opciones que admiten el valor <code>preemptionPolicy</code> como <code>PreemptLowerPriority</code> . Para obtener más información sobre la prioridad de los pods, consulte Prioridad y preferencia de pods en la Documentación de Kubernetes. • Escale verticalmente la instancia: para administrar sus recursos y realizar una selección óptima de instancias, consulte Administrar los recursos informáticos mediante nodos y Elegir un tipo de instancia de nodo óptimo de Amazon EC2 en la Guía del usuario de Amazon EKS.
Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods no están programados. Hay 0/x nodos disponibles: <code>x Too many pods. preemption: not eligible due to preemptionPolicy=Never</code> .	
Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods no están programados. Hay 0/x nodos disponibles: <code>1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never</code> .	

 Note

El mensaje muestra o/x porque GuardDuty solo informa del primer error encontrado. El número real de pods en ejecución en el daemonset de GuardDuty puede ser superior a 0.

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods tienen contenedores <code>CrashLoopBackOff: Completed</code> en espera	Puede ver los registros asociados al pod e identificar el problema. Para obtener información sobre cómo hacerlo, consulte Depurar pods en ejecución en la Documentación de Kubernetes. Use la siguiente lista de verificación para solucionar el problema de este complemento: • Valide que el monitoreo del tiempo de ejecución esté habilitado. • Valide que se cumple Requisitos previos para la compatibilidad con clústeres de Amazon EKS, como las distribuciones de sistema operativo verificadas y las versiones de Kubernetes compatibles. • Si administra el agente de seguridad de manera manual, confirme que ha creado un punto de conexión de VPC para todas las VPC. Al habilitar la configuración automatizada de GuardDuty, aún debe validar que se haya creado el punto de conexión de VPC. Por ejemplo, cuando se utiliza una VPC compartida en una configuración automática. Para validar esto, consulte Validar la configuración del punto de conexión de VPC. • Confirme que el agente de seguridad de GuardDuty puede resolver el DNS privado del punto de conexión de VPC de GuardDuty . Para conocer los puntos de conexión, consulte Nombres de DNS privados de

Error de creación o actualización del complemento	Pasos para la solución de problemas
	los puntos de conexión en Administrar los agentes de seguridad de GuardDuty. Para ello, puede utilizar cualquier herramienta nslookup en Windows o Mac o la herramienta dig en Linux. Cuando utilice nslookup, puede usar el siguiente comando después de reemplazar la región <i>us-west-2</i> con su región: <pre>nslookup guardduty-data. <i>us-west-2</i>.amazonaws.com</pre> • Valide que su política de puntos de conexión de VPC de GuardDuty o la política de control de servicios no afecten a la acción <code>guardduty:SendSecurityTelemetry</code>.

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods tienen contenedores <code>CrashLoopBackOff: Error</code> en espera	Puede ver los registros asociados al pod e identificar el problema. Para obtener información sobre cómo hacerlo, consulte Depurar pods en ejecución en la Documentación de Kubernetes. Una vez que se haya identificado el problema, use la siguiente lista de verificación para solucionarlo: • Valide que el monitoreo del tiempo de ejecución esté habilitado. • Valide que se cumple Requisitos previos para la compatibilidad con clústeres de Amazon EKS, como las distribuciones de sistema operativo verificadas y las versiones de Kubernetes compatibles. • El agente de seguridad de GuardDuty puede resolver el DNS privado del punto de conexión de VPC de GuardDuty. Para conocer los puntos de conexión, consulte Nombres de DNS privados de los puntos de conexión en Administrar los agentes de seguridad de GuardDuty.

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento de EKS: <pre>AdmissionRequestDenied : "validate .kyverno.svc-fail" de webhook de admisión denegó la solicitud: política DaemonSet/amazon-guardduty/aws- guardduty-agent para infracción de recursos: restrict-image-registries: autogen-va lidate-registries :...</pre>	1. El clúster de Amazon EKS o el administrador de seguridad deben revisar la política de seguridad que bloquea la actualización del complemento. 2. Debe desactivar el controlador (webhook) o hacer que el controlador acepte las solicitudes de Amazon EKS.
Problema con el complemento de EKS: <pre>ConfigurationConflict : se encontrar on conflictos al intentar la aplicación. No continuará debido al modo de resolución de conflictos. Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.tem plate.spec.containers[name= "aws-guardduty-agent"].image</pre>	Al crear o actualizar el complemento, indique la marca de resolución de conflictos <code>OVERWRITE</code>. Esto sobrescribirá potencialmente cualquier cambio que se haya realizado directamente en los recursos relacionados en Kubernetes a través de la API de Kubernetes. En primer lugar, se puede Quitar un complemento de Amazon EKS de un clúster y, a continuación, volver a instalarlo.

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento de EKS: <pre>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</pre>	Debe agregar el permiso que falta al <code>eks:addon-cluster-admin ClusterRoleBinding</code> manualmente. Agregue el siguiente <code>yaml</code> al <code>eks:addon-cluster-admin</code> : <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>
AddonUpdationFailed: EKSAaddonIssue: <pre>AccessDenied: namespaces\"amazon-guarddduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guarddduty\"</pre>	Ahora puede aplicar este <code>yaml</code> al clúster de Amazon EKS mediante el siguiente comando: <pre>kubectl apply -f eks-addon-cluster-admin.yaml</pre>

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento de EKS: <pre>AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must- have-label-owner] All namespaces must have an `owner` label</pre>	Debe desactivar el controlador o hacer que este acepte las solicitudes del clúster de Amazon EKS. Antes de crear o actualizar el complemento, también puede crear un espacio de nombres de GuardDuty y rotularlo como owner.
Problema con el complemento de EKS: - <pre>AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must- have-label-owner] All namespaces must have an `owner` label</pre>	Debe desactivar el controlador o hacer que este acepte las solicitudes del clúster de Amazon EKS. Antes de crear o actualizar el complemento, también puede crear un espacio de nombres de GuardDuty y rotularlo como owner.
Problema con el complemento de EKS: <pre>AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container- registries] container <aws-guar- dduty-agent> has an invalid image registry</pre>	Añada el registro de imágenes de GuardDuty a los allowed-container-registries en su controlador de admisión. Para obtener más información, consulte el repositorio ECR para EKS v1.8.1-eks-build.2 en Repositorio de Amazon ECR que aloja el agente de GuardDuty.

Configuración de la supervisión de la CPU y la memoria

Después de habilitar la Supervisión en tiempo de ejecución y evaluar que la cobertura del clúster esté en buen estado, podrá configurar y ver las métricas de Información.

Los siguientes temas resultan útiles a la hora de evaluar el rendimiento del agente implementado con respecto a los límites de CPU y memoria para el agente de GuardDuty.

Configurar la supervisión en el clúster de Amazon ECS

Los siguientes pasos de la Guía del usuario de Amazon CloudWatch pueden resultar útiles a la hora de evaluar el rendimiento del agente implementado con respecto a los límites de CPU y memoria para el agente de GuardDuty:

1. [Configurar Información de contenedores en Amazon ECS para métricas a nivel de clúster y de servicio](#)
2. [Métricas de Información de contenedores de Amazon ECS](#)

Configurar la supervisión en el clúster de Amazon EKS

Después de implementar el agente de seguridad de GuardDuty y evaluar que la cobertura del clúster está en buen estado, podrá configurar y ver las métricas de Información de Contenedores.

Evalúe el rendimiento del agente de seguridad

1. [Configurar Información de contenedores en Amazon EKS y Kubernetes](#) en la Guía del usuario de Amazon CloudWatch.
2. [Métricas de Información de contenedores de Amazon EKS y Kubernetes](#) en la Guía del usuario de Amazon CloudWatch

Administrar el rendimiento con la versión 1.5.0 o superior del agente de seguridad

Con la versión [v1.5.0 y posteriores](#) del agente de seguridad, cuando los datos indican que el agente de GuardDuty asociado está a punto de alcanzar los límites asignados, podrá configurar parámetros específicos. Para obtener más información, consulte [Configurar los parámetros del complemento de EKS](#).

Uso de VPC compartida con Runtime Monitoring

Runtime Monitoring de GuardDuty es compatible con Amazon Virtual Private Cloud (Amazon VPC) compartido para las Cuentas de AWS que pertenezca a la misma organización en AWS Organizations. Se puede usar la VPC compartida de dos maneras:

- Configuración automática del agente (recomendada): cuando GuardDuty administre de manera automática el agente de seguridad, también configurará la política de puntos de conexión de Amazon VPC. Esta política se basa en la configuración de VPC compartida de su organización.

Se debe habilitar la configuración automática del agente en la cuenta del propietario de la VPC compartida y en todas las cuentas participantes que compartirán esta VPC.

- Agente administrado de manera manual: al administrar de manera manual el agente de seguridad con una VPC compartida, debe actualizar la política de puntos de conexión de VPC para permitir que las cuentas correspondientes accedan a la VPC compartida. Para ello, se puede usar el ejemplo de política que se comparte en la siguiente sección [Funcionamiento](#).

En los escenarios de administración manual que involucran cuentas participantes para una VPC compartida, es posible que el estado de la cobertura no sea exacto. Para garantizar un estado actualizado de protección y cobertura de sus recursos, GuardDuty recomienda habilitar la configuración automática de agentes para todas las cuentas que utilizarán una VPC compartida.

Temas

- [Funcionamiento](#)
- [Requisitos previos para utilizar una VPC compartida](#)

Funcionamiento

Las Cuentas de AWS que pertenecen a la misma organización que la cuenta de propietario de la Amazon VPC compartida también pueden compartir el mismo punto de conexión de Amazon VPC. Cada una de las cuentas que utiliza la misma política de punto de conexión de Amazon VPC se denomina cuenta de AWS participante de la Amazon VPC compartida asociada.

El siguiente ejemplo muestra la política de punto de conexión de VPC predeterminada de la cuenta de propietario de la VPC compartida y la cuenta participante. `aws:PrincipalOrgID` mostrará el ID de la organización asociado al recurso de la VPC compartida. El uso de esta política se limita a las cuentas participantes presentes en la organización de la cuenta de propietario.

Example Ejemplo de política de punto de conexión de VPC compartida

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "*",
    "Resource": "*",
```

```
        "Effect": "Allow",
        "Principal": "*"
    },
    {
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalOrgID": "o-abcdef0123"
            }
        },
        "Action": "*",
        "Resource": "*",
        "Effect": "Deny",
        "Principal": "*"
    }
]
```

Con configuración automática de agentes GuardDuty

Cuando la cuenta de propietario de la VPC compartida habilita la Supervisión en tiempo de ejecución y la configuración automatizada del agente para cualquiera de los recursos (Amazon EKS o AWS Fargate (solo Amazon ECS)), todas las VPC compartidas adquieren la posibilidad de instalar automáticamente el punto de conexión de Amazon VPC compartida y el grupo de seguridad asociado en la cuenta de propietario de la VPC compartida. GuardDuty recupera el ID de organización asociado a la Amazon VPC compartida.

GuardDuty crea un punto de conexión de Amazon VPC cuando la cuenta de propietario de la VPC compartida o la cuenta participante lo necesita. Algunos ejemplos de casos en los que se necesita un punto de conexión de Amazon VPC son la habilitación de GuardDuty, la Supervisión en tiempo de ejecución, la Supervisión en tiempo de ejecución de EKS o el lanzamiento de una nueva tarea de Amazon ECS-Fargate. Cuando estas cuentas habilitan Runtime Monitoring y la configuración automatizada del agente para cualquier tipo de recurso, GuardDuty crea un punto de conexión de Amazon VPC y establece la política del punto de conexión con el mismo ID de organización que el de la cuenta de propietario de la VPC compartida. GuardDuty agrega una etiqueta `GuardDutyManaged` y la establece en `true` para el punto de conexión de Amazon VPC que GuardDuty crea. Si la cuenta de propietario de Amazon VPC compartida no ha habilitado la Supervisión en tiempo de ejecución o la configuración automatizada del agente para ninguno de los recursos, GuardDuty no establecerá la política de punto de conexión de Amazon VPC. Para obtener información sobre cómo configurar la Supervisión en tiempo de ejecución y administrar el agente de

seguridad automáticamente en la cuenta de propietario de la VPC compartida, consulte [Habilitar la Supervisión en tiempo de ejecución de GuardDuty](#).

Se utiliza con un agente administrado de manera manual

Cuando utilice una VPC compartida con un agente administrado de manera manual, compruebe que no haya una política de punto de conexión Deny explícita que bloquee una cuenta que necesite usar la VPC compartida. Esto evitará que el agente de seguridad envíe datos telemétricos a GuardDuty, lo que provocará una cobertura Unhealthy. Para configurar la política de puntos de conexión, consulte [Example shared VPC endpoint policy](#).

Es posible que la cobertura del tiempo de ejecución no sea precisa en situaciones como la falta de permisos para la VPC compartida. Puede monitorear de forma continua la cobertura de los recursos siguiendo los pasos correspondientes al tipo de recurso indicado [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Para garantizar la protección continua de sus recursos informáticos con Runtime Monitoring, GuardDuty recomienda habilitar la configuración automática de agentes para la cuenta propietaria de la VPC compartida y todas las cuentas participantes de sus recursos.

Requisitos previos para utilizar una VPC compartida

Como parte de una configuración inicial, siga los siguientes pasos en la Cuenta de AWS que desee que sea la propietaria de la VPC compartida:

1. Crear una organización: para crear una organización, siga los pasos que se indican en [Crear y administrar una organización](#) en la Guía del usuario de AWS Organizations.

Para obtener información sobre cómo agregar o eliminar cuentas de miembro, consulte [Administrar Cuentas de AWS en la organización](#).

2. Crear un recurso de VPC compartida: puede crear un recurso de VPC compartida desde la cuenta de propietario. Para obtener más información, consulte [Compartir las subredes de VPC con otras cuentas](#) en la Guía del usuario de Amazon VPC.

Requisitos previos específicos de la Supervisión en tiempo de ejecución de GuardDuty

La siguiente lista indica los requisitos previos específicos de GuardDuty:

- La cuenta de propietario de la VPC compartida y la cuenta participante pueden ser de diferentes organizaciones en GuardDuty. Sin embargo, deben pertenecer a la misma organización en AWS

Organizations. Esto es necesario para que GuardDuty cree un punto de conexión de Amazon VPC y un grupo de seguridad para la VPC compartida. Para obtener información sobre cómo funcionan las VPC compartidas, consulte [Compartir la VPC con otras cuentas](#) en la Guía del usuario de Amazon VPC.

- Habilitar la Supervisión en tiempo de ejecución o la Supervisión en tiempo de ejecución de EKS, y la configuración automatizada del agente de GuardDuty para cualquier recurso en la cuenta de propietario de la VPC compartida y en la cuenta participante. Para obtener más información, consulte [Habilitación de la supervisión en tiempo de ejecución](#).

Si ya ha completado estas configuraciones, continúe con el siguiente paso.

- Al trabajar con una tarea de Amazon EKS o de Amazon ECS (únicamente AWS Fargate), asegúrese de elegir el recurso de VPC compartida asociado a la cuenta de propietario y seleccione sus subredes.

Utilizar la Infraestructura como Código (IaC) con agentes de seguridad automatizados de GuardDuty

Utilice esta sección únicamente si la siguiente lista se aplica a su caso de uso:

- Utiliza herramientas de Infraestructura como Código (IaC), como AWS Cloud Development Kit (AWS CDK) y Terraform, para administrar los recursos de AWS, y
- Necesita habilitar la configuración automatizada del agente de GuardDuty para uno o varios tipos de recursos: Amazon EKS, Amazon EC2 o Amazon ECS-Fargate.

Información general sobre el gráfico de dependencia de recursos de IaC

Cuando se habilita la configuración automatizada del agente de GuardDuty para un tipo de recurso, GuardDuty crea automáticamente un punto de conexión de VPC y un grupo de seguridad asociado a este punto de conexión de VPC, e instala el agente de seguridad para este tipo de recurso. De forma predeterminada, GuardDuty eliminará el punto de conexión de VPC y el grupo de seguridad asociado solo después de que desactive la Supervisión en tiempo de ejecución. Para obtener más información, consulte [Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución](#).

Cuando utiliza una herramienta de IaC, esta mantiene un gráfico de dependencia de los recursos. Cuando se eliminan recursos con la herramienta de IaC, únicamente se eliminan los recursos de

los que se puede hacer un seguimiento como parte del gráfico de dependencia de recursos. Es posible que las herramientas de IaC no tengan conocimiento de los recursos que se crean fuera de su configuración especificada. Por ejemplo, crea una VPC con una herramienta de IaC y luego agrega un grupo de seguridad a esta VPC mediante la consola de AWS o una operación de la API. En el gráfico de dependencias de recursos, el recurso de la VPC que crea dependerá del grupo de seguridad asociado. Si elimina este recurso de la VPC con la herramienta de IaC, se producirá un error. La forma de evitar este error es eliminar manualmente el grupo de seguridad asociado o actualizar la configuración de IaC para incluir este recurso agregado.

Problema común: eliminar recursos en IaC

Al utilizar la configuración automatizada del agente de GuardDuty, es posible que desee eliminar un recurso (Amazon EKS, Amazon EC2 o Amazon ECS-Fargate) que haya creado mediante una herramienta de IaC. Sin embargo, este recurso depende de un punto de conexión de VPC que GuardDuty creó. Esto impide que la herramienta IaC elimine el recurso por sí misma y requiere que desactive la Supervisión en tiempo de ejecución, que además elimina el punto de conexión de VPC automáticamente.

Por ejemplo, cuando intenta eliminar el punto de conexión de VPC que GuardDuty creó en su nombre, se producirá un error similar al de los siguientes ejemplos.

Example

Ejemplo de error al usar CDK

```
The following resource(s) failed to delete:
[mycdkvpccapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpccapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
HandlerErrorCode: InvalidRequest)
```

Example

Ejemplo de error al usar 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
```

Solución: evite el problema de eliminación de recursos

Esta sección ayuda a administrar el punto de conexión de VPC y el grupo de seguridad independientemente de GuardDuty.

Para adquirir la propiedad completa de los recursos configurados mediante la herramienta de laC, siga los siguientes pasos en el orden indicado:

1. Cree una VPC. Para autorizar el permiso de entrada, asocie un punto de conexión de VPC de GuardDuty con el grupo de seguridad, a esta VPC.
2. Habilitar la configuración automatizada del agente de GuardDuty para el tipo de recurso

Después de completar los pasos anteriores, GuardDuty no creará su propio punto de conexión de VPC y reutilizará el que usted creó mediante la herramienta de laC.

Para obtener información sobre cómo crear una VPC propia, consulte [Crear una VPC únicamente](#) en las Puertas de enlace de tránsito de Amazon VPC. Para obtener información sobre cómo crear un punto de conexión de VPC, consulte la siguiente sección para el tipo de recurso:

- Para Amazon EC2, consulte [Requisito previo: crear manualmente el punto de conexión de Amazon VPC](#).
- Para Amazon EKS, consulte [Requisito previo: crear un punto de conexión de Amazon VPC](#).

Tipos de eventos de tiempo de ejecución recopilados que utiliza GuardDuty

El agente de seguridad de GuardDuty recopila los siguientes tipos de eventos y los envía al backend de GuardDuty para la detección y el análisis de amenazas. GuardDuty no hace que estos eventos sean accesibles para usted. Si GuardDuty detecta una amenaza potencial y genera un [Tipos de resultados de la supervisión en tiempo de ejecución](#), puede ver los detalles del resultado correspondiente.

Para obtener información sobre cómo GuardDuty utiliza los tipos de eventos recopilados en la Supervisión en tiempo de ejecución, consulte [Optar por no utilizar sus datos para mejorar el servicio](#).

Eventos de procesos

Los eventos de los procesos representan información asociada a los procesos que se ejecutan en las instancias de Amazon EC2 y las cargas de trabajo de contenedores. La siguiente tabla incluye los nombres de los campos y las descripciones de los eventos de los procesos que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Process name	Nombre del proceso observado.
Ruta de proceso	Ruta absoluta del ejecutable del proceso.
ID de proceso	ID asignado al proceso por el sistema operativo.
PID de espacio de nombres	ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID de nivel de host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
ID de usuario del proceso	ID único del usuario que ha ejecutado el proceso.
UUID de proceso	ID único asignado al proceso por GuardDuty.
GID de proceso	ID del proceso del grupo de procesos.
EGID de proceso	ID del grupo efectivo del grupo de procesos.
EUID de proceso	ID del usuario efectivo del proceso.
Nombre de usuario de proceso	Nombre del usuario que ha ejecutado el proceso.
Hora de inicio de proceso	Hora de creación del proceso. Este campo está en formato de cadena de fecha UTC (2023-03-22T19:37:20.168Z).

Nombre del campo	Descripción
SHA-256 de ejecutable de proceso	Hash SHA256 del ejecutable del proceso.
Ruta de script de proceso	Ruta del archivo del script que se ha ejecutado.
Variable de entorno de proceso	Variable de entorno puesta a disposición del proceso. Solo se recopilan LD_PRELOAD y LD_LIBRARY_PATH .
Directorio de trabajo actual (PWD) de proceso	Directorio de trabajo actual del proceso.
Proceso principal	Detalles del proceso principal. Un proceso principal es un proceso que creó el proceso observado.
Argumentos de línea de comandos	Argumentos de línea de comandos proporcionados en el momento de la ejecución del proceso. Es posible que este campo contenga datos confidenciales del cliente.
Actualmente, este campo está limitado a versiones específicas del agente correspondientes al tipo de recurso: • Fargate (solo Amazon ECS) con la versión 1.0.0 o posterior del agente de seguridad de GuardDuty. • Instancias de Amazon EC2 con la versión 1.0.0 o posterior del agente de seguridad de GuardDuty. • Los clústeres de Amazon EKS con la versión 1.4.0 o posterior del agente de seguridad. Para obtener más información, consulte Versiones del agente de seguridad de GuardDuty.	

Eventos de contenedores

Los eventos de contenedores representan información asociada a las actividades de las cargas de trabajo de los contenedores. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de la carga de trabajo del contenedor que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Nombre de contenedor	Nombre del contenedor. Cuando está disponible, este campo muestra el valor de la etiqueta <code>io.kubernetes.container.name</code> .
UID de contenedor	ID único del contenedor asignado por el tiempo de ejecución del contenedor.
Tiempo de ejecución de contenedor	Tiempo de ejecución del contenedor (por ejemplo, <code>docker</code> o <code>containerd</code>) utilizado para ejecutar el contenedor.
ID de imagen de contenedor	ID de la imagen del contenedor.
Nombre de imagen de contenedor	Nombre de la imagen del contenedor.

Eventos de tareas de AWS Fargate (solo en Amazon ECS)

Los eventos de tareas de Fargate-Amazon ECS representan actividades asociadas a tareas de Amazon ECS que se ejecutan en computaciones de Fargate. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de tareas de Amazon ECS-Fargate que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Nombre de recurso de Amazon (ARN) de la tarea	El ARN de la tarea.
Nombre del clúster	El nombre del clúster de Amazon ECS.

Nombre del campo	Descripción
Apellido	El apellido de la definición de la tarea. El <code>family</code> se utiliza como nombre para la definición de la tarea que se utiliza para lanzar la tarea.
Nombre del servicio	El nombre del servicio de Amazon ECS, si la tarea se lanzó como parte de un servicio.
Tipo de lanzamiento	La infraestructura en la que se ejecuta la tarea. Para la Supervisión en tiempo de ejecución con el tipo de recurso como <code>ECSCluster</code> , el tipo de lanzamiento puede ser <code>EC2</code> o <code>FARGATE</code> .
CPU	La cantidad de unidades de CPU utilizadas por la tarea, tal como se expresa en la definición de la tarea.

Eventos de pod de Kubernetes

En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos del pod de Kubernetes que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
ID de pod	ID del pod de Kubernetes.
Nombre de pod	Nombre del pod de Kubernetes.
Espacio de nombres de pod	Nombre del espacio de nombres de Kubernetes al que pertenece la carga de trabajo de Kubernetes.
Nombre de clúster de Kubernetes	Nombre del clúster de Kubernetes.

Eventos del sistema de nombres de dominio (DNS)

Los eventos del sistema de nombres de dominio (DNS) incluyen detalles de las consultas DNS realizadas por los tipos de recursos y las respuestas correspondientes. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de DNS que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4.
ID de dirección	ID de la dirección de conexión.
Número de protocolo	Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).
IP de punto de conexión remoto de DNS	IP remota de la conexión.
Puerto de punto de conexión remoto de DNS	Número del puerto de la conexión.
IP de punto de conexión local de DNS	IP local de la conexión.
Puerto de punto de conexión local de DNS	Número del puerto de la conexión.
Carga de DNS	Carga de los paquetes de DNS que contiene consultas y respuestas de DNS.

Eventos abiertos

Los eventos de apertura están asociados al acceso y modificación de archivos. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de apertura que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Ruta de archivo	Ruta del archivo que se abre en este evento.
Indicadores	Describe el modo de acceso a archivos, como solo lectura, solo escritura y lectura-escritura.

Evento de carga de módulo

En la siguiente tabla se incluyen el nombre del campo y la descripción del evento del módulo de carga que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Nombre de módulo	Nombre del módulo cargado en el kernel.

Eventos de Mprotect

Los eventos de Mprotect proporcionan información sobre los cambios en la configuración de protección de memoria de los procesos que se ejecutan en los sistemas supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de Mprotect que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Rango de direcciones	Rango de direcciones para el que se modificaron las protecciones de acceso.
Regiones de memoria	Especifica la región del espacio de direcciones de un proceso, como la pila y el montón.

Nombre del campo	Descripción
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Eventos de montaje

Los eventos de montaje proporcionan información asociada al montaje y desmontaje de sistemas de archivos en el recurso supervisado. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de montaje que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Destino de montaje	Ruta en la que se monta el origen del montaje.
Origen de montaje	Ruta del host que se monta en el destino de montaje.
Tipo de sistema de archivos	Representa el tipo de sistema de archivos montado.
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Eventos de enlace

Los eventos de enlaces proporcionan visibilidad de las actividades de administración de enlaces del sistema de archivos en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de enlaces que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Ruta de enlace	Ruta en la que se crea el enlace físico.
Ruta de destino	Ruta del archivo al que apunta el enlace físico.

Eventos de enlace simbólico

Los eventos de enlaces simbólicos (symlink) proporcionan visibilidad de las actividades de administración de enlaces simbólicos del sistema de archivos en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de enlaces simbólicos que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Ruta de enlace	Ruta en la que se crea el enlace simbólico.
Ruta de destino	Ruta del archivo al que apunta el enlace simbólico.

Eventos duplicados

Los eventos de duplicación (dup) proporcionan visibilidad sobre la duplicación de descriptors de archivo por parte de los procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de duplicación que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Descriptor de archivo antiguo	Descriptor de archivo que representa un objeto de archivo abierto.
Descriptor de archivo nuevo	Descriptor de archivo nuevo que es un duplicado del descriptor de archivo antiguo. Tanto el descriptor de archivo antiguo como el nuevo representan el mismo objeto de archivo abierto.
IP de punto de conexión remoto de duplicación	Dirección IP remota del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.
Puerto de punto de conexión remoto de duplicación	Puerto remoto del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.

Nombre del campo	Descripción
IP de punto de conexión local de duplicación	Dirección IP local del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.
Puerto de punto de conexión local de duplicación	Puerto local del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.

Evento de mapa de memoria

En la siguiente tabla se incluye el nombre del campo y la descripción de los eventos del mapa de memoria que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Ruta de archivo	Ruta del archivo al que se asigna la memoria.

Eventos de socket

Los eventos de socket proporcionan información sobre las conexiones de socket de red utilizadas en las actividades de los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de socket que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para la versión de IP del protocolo 4.
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.
Número de protocolo	Especifica un protocolo concreto de la familia de direcciones. Por lo general, hay un único protocolo en las familias de

Nombre del campo	Descripción
	direcciones. Por ejemplo, la familia de direcciones AF_INET solo tiene el protocolo de IP.

Eventos de conexión

Los eventos de conexión proporcionan visibilidad de las conexiones de red establecidas por los procesos en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de conexión que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4.
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.
Número de protocolo	Especifica un protocolo concreto de la familia de direcciones. Por lo general, hay un único protocolo en las familias de direcciones. Por ejemplo, la familia de direcciones AF_INET solo tiene el protocolo de IP.
Ruta de archivo	Ruta del archivo de socket si la familia de direcciones es AF_UNIX.
IP de punto de conexión remoto	IP remota de la conexión.
Puerto de punto de conexión remoto	Número del puerto de la conexión.
IP de punto de conexión local	IP local de la conexión.

Nombre del campo	Descripción
Puerto de punto de conexión local	Número del puerto de la conexión.

Eventos de Readv de VM de proceso

Los eventos de procesos de lectura de memoria virtual (VM readv) proporcionan visibilidad de las operaciones de lectura realizadas por los procesos en sus propias regiones de memoria virtual. La siguiente tabla incluye los nombres de los campos y las descripciones de los eventos de procesos de lectura de memoria virtual que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Indicadores	Representa las opciones que controlan el comportamiento de este evento.
PID de destino	ID del proceso desde el que se lee la memoria.
UUID de proceso de destino	ID único del proceso de destino.
Ruta de ejecutable de destino	Ruta absoluta del archivo ejecutable del proceso de destino.

Eventos de Writev de VM de proceso

Los eventos de procesos de escritura de memoria virtual (VM writev) proporcionan visibilidad de las operaciones de escritura realizadas por los procesos en sus propias regiones de memoria virtual. La siguiente tabla incluye los nombres de los campos y las descripciones de los eventos de los procesos de escritura de memoria virtual que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Nombre del campo	Descripción
PID de destino	ID del proceso en el que se escribe la memoria.
UUID de proceso de destino	ID único del proceso de destino.
Ruta de ejecutable de destino	Ruta absoluta del archivo ejecutable del proceso de destino.

Eventos de rastreo de procesos (Ptrace)

La llamada al sistema de rastreo de procesos (Ptrace) es un mecanismo de depuración y rastreo que permite a un proceso (rastreador) observar y controlar la ejecución de otro proceso (rastreado). Esto proporciona al rastreador la capacidad de inspeccionar y modificar la memoria, los registros y el flujo de ejecución del proceso de destino.

Los eventos ptrace proporcionan visibilidad sobre el uso de la llamada al sistema ptrace por parte de los procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos ptrace que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
PID de destino	ID del proceso de destino.
UUID de proceso de destino	ID único del proceso de destino.
Ruta de ejecutable de destino	Ruta absoluta del archivo ejecutable del proceso de destino.
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Enviar de vinculación

Los eventos de vinculación proporcionan visibilidad sobre la vinculación de sockets de red por parte de los procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de circulación que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4.
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.
Número de protocolo	Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).
IP de punto de conexión local	IP local de la conexión.
Puerto de punto de conexión local	Número del puerto de la conexión.

Eventos de escucha

Los eventos de escucha proporcionan visibilidad sobre el estado de escucha de los sockets de red, e indican si un socket de red está listo o no para aceptar conexiones entrantes. Un proceso que se ejecuta en el recurso supervisado establece el socket de red en estado de escucha. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de escucha que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4.
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.
Número de protocolo	Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).
IP de punto de conexión local	IP local de la conexión.

Nombre del campo	Descripción
Puerto de punto de conexión local	Número del puerto de la conexión.

Eventos de cambio de nombre

Los eventos de cambio de nombre proporcionan información sobre el cambio de nombre de archivos y directorios por parte de procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de cambio de nombre que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Ruta de archivo	Ruta donde se encuentra el archivo cuyo nombre se ha cambiado.
Destino	La nueva ruta del archivo.

Eventos de establecimiento de ID de usuario (UID)

Los eventos de establecimiento de ID de usuario (UID) proporcionan visibilidad de los cambios realizados en el ID de usuario (UID) asociado a los procesos en ejecución en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de establecimiento de ID de usuario (UID) que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Nuevo EUID	El nuevo ID de usuario efectivo del proceso.
Nuevo UID	El nuevo ID de usuario del proceso.

Eventos chmod

Los eventos chmod proporcionan visibilidad de los cambios en los permisos (modo) de archivos y directorios en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos chmod que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

Nombre del campo	Descripción
Ruta de archivo	Ruta del archivo que invoca este evento.
Modo de archivo	Los permisos de acceso actualizados para el archivo asociado.

Repositorio de Amazon ECR que aloja el agente de GuardDuty

En las siguientes secciones se enumeran los repositorios de Amazon Elastic Container Registry (Amazon ECR) en los que GuardDuty aloja el agente de seguridad que se implementa en los clústeres de Amazon EKS y Amazon ECS.

El requisito previo para [Requisitos previos para el acceso a imágenes de contenedores](#) requiere que proporcione un rol de ejecución de tareas que tenga determinados permisos de Amazon Elastic Container Registry (Amazon ECR). Para restringir aún más estos permisos, puede agregar el URI del repositorio de Amazon ECR que aloja el agente de GuardDuty para los recursos de Fargate-Amazon ECS.

Repositorio de ECR para las versiones 1.11.0 a 1.8.1 del agente EKS (eks.build.2)

Al habilitar la configuración automática de GuardDuty para Runtime Monitoring de EKS, GuardDuty implementará esta versión del agente en sus clústeres de Amazon EKS. Para obtener información acerca de cómo habilitar el agente automatizado, consulte [Administración automática del agente de seguridad para los recursos de Amazon EKS](#).

En la siguiente tabla se muestran los URI del repositorio de Amazon ECR donde se alojan las versiones del agente de seguridad de GuardDuty 1.11.0.eks.build.2, 1.10.0.eks.build.2, 1.9.0.eks.build.2 y 1.8.0.eks.build.2 para Amazon EKS.

Región de AWS	URI del repositorio de Amazon ECR
Oeste de EE. UU. (Oregón)	602401143452.dkr.ecr.us-west-2.amazonaws.com
	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europa (París)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia-Pacífico (Mumbai)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia-Pacífico (Hyderabad)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canadá (centro)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Oeste de Canadá (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
	—
Medio Oriente (EAU)	759879836304.dkr.ecr.me-central-1.amazonaws.com

Región de AWS	URI del repositorio de Amazon ECR
	<code>601769779514.dkr.ecr.me-central-1.amazonaws.com</code>
Europa (Londres)	<code>602401143452.dkr.ecr.eu-west-2.amazonaws.com</code>
	<code>109118265657.dkr.ecr.eu-west-2.amazonaws.com</code>
Oeste de EE. UU. (Norte de California)	<code>602401143452.dkr.ecr.us-west-1.amazonaws.com</code>
	<code>373421517865.dkr.ecr.us-west-1.amazonaws.com</code>
Este de EE. UU. (Norte de Virginia)	<code>602401143452.dkr.ecr.us-east-1.amazonaws.com</code>
	<code>031903291036.dkr.ecr.us-east-1.amazonaws.com</code>
Este de EE. UU. (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>
América del Sur (São Paulo)	<code>602401143452.dkr.ecr.sa-east-1.amazonaws.com</code>
	<code>941219317354.dkr.ecr.sa-east-1.amazonaws.com</code>

Región de AWS	URI del repositorio de Amazon ECR
Europa (Estocolmo)	<code>602401143452.dkr.ecr.eu-nor th-1.amazonaws.com</code>
	<code>366771026645.dkr.ecr.eu-nor th-1.amazonaws.com</code>
Europa (Fráncfort)	<code>602401143452.dkr.ecr.eu-cen tral-1.amazonaws.com</code>
	<code>409493279830.dkr.ecr.eu-cen tral-1.amazonaws.com</code>
Europa (Zúrich)	<code>900612956339.dkr.ecr.eu-cen tral-2.amazonaws.com</code>
	<code>718440343717.dkr.ecr.eu-cen tral-2.amazonaws.com</code>
Asia-Pacífico (Singapur)	<code>602401143452.dkr.ecr.ap-sou theast-1.amazonaws.com</code>
	<code>584580519942.dkr.ecr.ap-sou theast-1.amazonaws.com</code>
Asia-Pacífico (Sídney)	<code>602401143452.dkr.ecr.ap-sou theast-2.amazonaws.com</code>
	<code>011662287384.dkr.ecr.ap-sou theast-2.amazonaws.com</code>
Asia-Pacífico (Yakarta)	<code>296578399912.dkr.ecr.ap-sou theast-3.amazonaws.com</code>
	<code>617474730032.dkr.ecr.ap-sou theast-3.amazonaws.com</code>
Asia-Pacífico (Tokio)	<code>602401143452.dkr.ecr.ap-nor theast-1.amazonaws.com</code>

Región de AWS	URI del repositorio de Amazon ECR
Asia-Pacífico (Seúl)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia-Pacífico (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia-Pacífico (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Medio Oriente (Baréin)	558608220178.dkr.ecr.me-south-1.amazonaws.com
	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milán)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (España)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
	531047660167.dkr.ecr.eu-south-2.amazonaws.com

Región de AWS	URI del repositorio de Amazon ECR
África (Ciudad del Cabo)	877085696533.dkr.ecr.af-south-1.amazonaws.com
	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia-Pacífico (Melbourne)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	066635153087.dkr.ecr.il-central-1.amazonaws.com
	292660727137.dkr.ecr.il-central-1.amazonaws.com
Asia-Pacífico (Malasia)	151610086707.dkr.ecr.ap-southeast-5.amazonaws.com
Asia-Pacífico (Tailandia)	121268973566.dkr.ecr.ap-southeast-7.amazonaws.com
México (central)	730335286997.dkr.ecr.mx-central-1.amazonaws.com
Asia-Pacífico (Taipéi)	533267051163.dkr.ecr.ap-east-2.amazonaws.com

Repositorio de ECR para la versión 1.8.1 del agente de EKS (**eks.build.1**)

En esta sección se proporciona el repositorio de Amazon ECR para la versión 1.8.1 del agente Amazon EKS (v1.8.1-eks-build.1). Si utiliza la versión 1.8.1-eks-build.1, GuardDuty recomienda cambiar a la versión predeterminada del agente, que suele ser la versión más reciente del agente. Para ello, identifique el agente más reciente de [Se lanzaron versiones de agente publicadas para](#)

[los recursos de Amazon EKS](#) y, a continuación, lleve a cabo los pasos que se indican en [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#).

En la siguiente tabla se muestran los URI del repositorio de Amazon ECR donde se aloja la versión 1.8.1-eks-build.1 del agente de seguridad GuardDuty para Amazon EKS.

Región de AWS	URI del repositorio de Amazon ECR
Oeste de EE. UU. (Oregón)	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europa (París)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia-Pacífico (Mumbai)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia-Pacífico (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canadá (centro)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Medio Oriente (EAU)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (Londres)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
Oeste de EE. UU. (Norte de California)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Este de EE. UU. (Norte de Virginia)	031903291036.dkr.ecr.us-east-1.amazonaws.com
Este de EE. UU. (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irlanda)	673884943994.dkr.ecr.eu-west-1.amazonaws.com

Región de AWS	URI del repositorio de Amazon ECR
América del Sur (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Estocolmo)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Fráncfort)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zúrich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia-Pacífico (Singapur)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia-Pacífico (Sídney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia-Pacífico (Yakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia-Pacífico (Tokio)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia-Pacífico (Seúl)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia-Pacífico (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia-Pacífico (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Medio Oriente (Baréin)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milán)	528450769569.dkr.ecr.eu-south-1.amazonaws.com

Región de AWS	URI del repositorio de Amazon ECR
Europa (España)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
África (Ciudad del Cabo)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia-Pacífico (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repositorio de ECR para el agente de GuardDuty en AWS Fargate (solo Amazon ECS)

Como requisito previo para utilizar Runtime Monitoring para Amazon ECS-Fargate, se debe [Requisitos previos para el acceso a imágenes de contenedores](#). La imagen del contenedor sidecar del agente de GuardDuty se almacena en Amazon ECR y las capas de imágenes se almacenan en Amazon S3. Para obtener más información, consulte [Cómo funciona la supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#).

En la siguiente tabla aparecen los repositorios de Amazon ECR que alojan el agente de GuardDuty para AWS Fargate (solo Amazon ECS) para cada Región de AWS.

Región de AWS	URI del repositorio de Amazon ECR
Oeste de EE. UU. (Oregón)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guard-duty-agent-fargate
Europa (París)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guard-duty-agent-fargate

Región de AWS	URI del repositorio de Amazon ECR
Asia-Pacífico (Mumbai)	251508486986.dkr.ecr.ap-sou th-1.amazonaws.com/aws-guar dduty-agent-fargate
Asia-Pacífico (Hyderabad)	950823858135.dkr.ecr.ap-sou th-2.amazonaws.com/aws-guar dduty-agent-fargate
Canadá (centro)	354763396469.dkr.ecr.ca-cen tral-1.amazonaws.com/aws-gu ardduty-agent-fargate
Medio Oriente (EAU)	000014521398.dkr.ecr.me-cen tral-1.amazonaws.com/aws-gu ardduty-agent-fargate
Europa (Londres)	892757235363.dkr.ecr.eu-wes t-2.amazonaws.com/aws-guard duty-agent-fargate
Oeste de EE. UU. (Norte de California)	684579721401.dkr.ecr.us-wes t-1.amazonaws.com/aws-guard duty-agent-fargate
Este de EE. UU. (Norte de Virginia)	593207742271.dkr.ecr.us-eas t-1.amazonaws.com/aws-guard duty-agent-fargate
Este de EE. UU. (Ohio)	307168627858.dkr.ecr.us-eas t-2.amazonaws.com/aws-guard duty-agent-fargate
Europa (Irlanda)	694911143906.dkr.ecr.eu-wes t-1.amazonaws.com/aws-guard duty-agent-fargate

Región de AWS	URI del repositorio de Amazon ECR
América del Sur (São Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Estocolmo)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Fráncfort)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Zúrich)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Singapur)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Sídney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Yakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Tokio)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Seúl)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate

Región de AWS	URI del repositorio de Amazon ECR
Asia-Pacífico (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente (Baréin)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Milán)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (España)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
África (Ciudad del Cabo)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
Israel (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Malasia)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate

Región de AWS	URI del repositorio de Amazon ECR
Asia-Pacífico (Tailandia)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate
Oeste de Canadá (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate
México (central)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Taipéi)	259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate

Dos agentes de seguridad en el mismo host subyacente

Las instancias de Amazon EC2 pueden admitir varios tipos de cargas de trabajo. Cuando se configura un agente de seguridad automatizado en una instancia de Amazon EC2, es posible que la misma instancia de EC2 tenga otro agente de seguridad a través de EKS.

Descripción general

Considere un escenario en el que ha habilitado la Supervisión en tiempo de ejecución. Ahora, habilita el agente automatizado para Amazon EKS a través de GuardDuty. Además, ha habilitado el agente automatizado para Amazon EC2. Puede ocurrir que el mismo host subyacente se instale con dos agentes de seguridad: uno para Amazon EKS y otro para Amazon EC2. Esto podría dar lugar a que dos agentes de seguridad se ejecuten en el mismo host, recopilen eventos en tiempo de ejecución, los envíen a GuardDuty y, potencialmente, generen resultados duplicados.

Impact

- Cuando hay más de un agente de seguridad en ejecución en el mismo host, es posible que la cuenta experimente el doble de demanda de CPU y memoria. Para obtener más información

acerca de los límites de CPU y memoria para cada tipo de recurso, consulte [Requisitos previos](#) para ese recurso.

- GuardDuty ha diseñado la característica de Supervisión en tiempo de ejecución para garantizar que, incluso si dos agentes de seguridad recopilan eventos en tiempo de ejecución del mismo host subyacente, la cuenta solo incurra en un cargo por una única secuencia de eventos en tiempo de ejecución.

Cómo GuardDuty gestiona a varios agentes

GuardDuty detecta cuando dos agentes de seguridad se ejecutan en el mismo host y designa solo a uno de los dos como el agente de seguridad que recopila activamente los eventos en tiempo de ejecución. El segundo agente consumirá un mínimo de recursos del sistema para evitar cualquier impacto en el rendimiento de las aplicaciones.

GuardDuty considera las siguientes situaciones:

- Cuando una instancia de EC2 entra en el ámbito tanto de los agentes de seguridad de Amazon EKS como de Amazon EC2, el agente de seguridad de EKS tiene prioridad. Esto se aplicará únicamente si utiliza la versión 1.1.0 o posterior del agente de seguridad para Amazon EC2. Las versiones más antiguas de los agentes seguirán en ejecución y aún recopilarán eventos en tiempo de ejecución, ya que las versiones más antiguas no se ven afectadas por la priorización.
- Cuando tanto Amazon EKS como Amazon EC2 tienen agentes de seguridad administrados de GuardDuty y la instancia de Amazon EC2 también es administrada por SSM, ambos agentes de seguridad se instalarán a nivel de host. Una vez instalados los agentes, GuardDuty decidirá qué agente de seguridad se mantendrá en ejecución. Cuando ambos agentes de seguridad se ejecutan, finalmente solo uno de ellos recopila eventos en tiempo de ejecución.
- Si los agentes de seguridad asociados a EC2 y EKS se ejecutan al mismo tiempo, es posible que GuardDuty genere resultados duplicados únicamente durante el periodo de superposición.

Esto puede ocurrir si:

- Los agentes de seguridad tanto para EC2 como para EKS se configuran a través de GuardDuty (automáticamente), o bien
- El recurso de Amazon EKS cuenta con un agente de seguridad automatizado.
- Cuando el agente de seguridad de EKS se encuentra en ejecución, si se implementa manualmente el agente de seguridad de EC2 en el mismo host subyacente y se cumplen todos los requisitos previos, es posible que GuardDuty no instale un segundo agente de seguridad.

Supervisión en tiempo de ejecución de EKS en GuardDuty

La supervisión en tiempo de ejecución de EKS proporciona una cobertura de detección de amenazas en tiempo de ejecución para los nodos y contenedores de Amazon Elastic Kubernetes Service (Amazon EKS) de su entorno de AWS. La supervisión en tiempo de ejecución de EKS utiliza un agente de seguridad de GuardDuty que agrega visibilidad en tiempo de ejecución a las cargas de trabajo individuales de EKS (por ejemplo, el acceso a los archivos, la ejecución de procesos y las conexiones de red). El agente de seguridad de GuardDuty ayuda a GuardDuty a identificar contenedores específicos dentro de sus clústeres de EKS que estén potencialmente en peligro. También puede detectar los intentos de escalar los privilegios de un contenedor individual al host de EC2 subyacente y al entorno de AWS en general.

Con la disponibilidad de la Supervisión en tiempo de ejecución, GuardDuty ha consolidado la experiencia de la consola para la Supervisión en tiempo de ejecución de EKS en la Supervisión en tiempo de ejecución. GuardDuty no migrará automáticamente la configuración de la Supervisión en tiempo de ejecución de EKS en su nombre. Para ello, es necesario que actúe. Si desea continuar con el uso de la Supervisión en tiempo de ejecución de EKS únicamente, puede utilizar las API o la AWS CLI para comprobar y actualizar el estado de la configuración existente para la Supervisión en tiempo de ejecución de EKS. Sin embargo, GuardDuty recomienda [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#) y utilizar la Supervisión en tiempo de ejecución para supervisar los clústeres de Amazon EKS.

Temas

- [Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas \(API\)](#)
- [Configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente \(API\)](#)
- [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#)

Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas (API)

En entornos con varias cuentas, solo la cuenta de administrador delegado de GuardDuty puede habilitar o deshabilitar la Supervisión en tiempo de ejecución de EKS para las cuentas de miembro, así como manejar la administración de agentes de GuardDuty para los clústeres de EKS que pertenecen a las cuentas de miembro de la organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado

de GuardDuty administra las cuentas de miembro a través de AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

Configurar la Supervisión en tiempo de ejecución de EKS para la cuenta de administrador delegado de GuardDuty

En esta sección se indican los pasos a seguir para configurar la Supervisión de tiempo de ejecución de EKS y administrar el agente de seguridad de GuardDuty para los clústeres de EKS que pertenecen a la cuenta de administrador delegado de GuardDuty.

Según los [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (supervisión de todos los clústeres de EKS)	Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre>'[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3.  Note Agregue siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor de STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>. Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el par <code>GuardDutyManaged -true</code>. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita <code>EKS_RUNTIME_MONITORING</code> y se deshabilita <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración manual del agente de seguridad	Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>. Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita <code>EKS_RUNTIME_MONITORING</code> y se deshabilita <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" : " ENABLED"}]]'</pre> Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Habilitación automática de la supervisión en tiempo de ejecución de EKS para todas las cuentas de miembros

En esta sección se incluyen los pasos para habilitar la Supervisión en tiempo de ejecución de EKS y administrar el agente de seguridad para todas las cuentas de miembro. Esto incluye la cuenta de administrador delegado de GuardDuty, las cuentas de miembro existentes y las nuevas cuentas que se unan a la organización.

Según los [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (supervisión de todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNT</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty

Pasos

```
IME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'
```

Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -false. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> . • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn : <pre data-bbox="634 1272 1406 1430">"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 Agregue siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor de STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y 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 También puede pasar una lista de ID de cuentas separadas por un espacio.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinación de clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -true. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> . • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn : <pre data-bbox="639 1283 1406 1434">"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. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de

Enfoque preferido para administrar el agente de seguridad de GuardDuty

Pasos

Amazon EKS que se hayan etiquetado con el par GuardDuty Managed -true.

También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita 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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de UnprocessedAccounts vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración manual del agente de seguridad	Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita 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> Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Configuración de la supervisión en tiempo de ejecución de EKS para todas las cuentas de miembros activas existentes

Esta sección incluye los pasos para habilitar la Supervisión en tiempo de ejecución de EKS y administrar el agente de seguridad GuardDuty para las cuentas de miembro activas existentes en la organización.

Según los [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (supervisión de todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y 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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty

Pasos



Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -false. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> . • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn : <pre data-bbox="639 1283 1406 1430">"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 Agregue siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor de STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y 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 También puede pasar una lista de ID de cuentas separadas por un espacio.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determina dos clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -true. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> . • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> . • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code> . • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn : <pre data-bbox="639 1283 1406 1434">"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. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.

Enfoque preferido para administrar el agente de seguridad de GuardDuty

Pasos

GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el par GuardDuty Managed `-true`.

También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración manual del agente de seguridad	- Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 5555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] }]'</pre> - Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Habilitación automática de la supervisión en tiempo de ejecución de EKS para los nuevos miembros

La cuenta de administrador delegado de GuardDuty puede habilitar automáticamente la Supervisión en tiempo de ejecución de EKS y elegir un enfoque para administrar el agente de seguridad de GuardDuty para las nuevas cuentas que se unan a su organización.

Según los [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (supervisión de todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilitan EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. <pre data-bbox="651 1709 1507 1879">aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "Addition</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre data-bbox="654 300 1503 401">alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3.  Note Agregue siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor de STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilitan EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. <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> Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el par GuardDutyManaged -true. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. <pre data-bbox="716 1787 1508 1873">aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre data-bbox="716 304 1507 520">bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración manual del agente de seguridad	1. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre data-bbox="716 304 1507 401">ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema. 2. Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Habilitación de la Supervisión en tiempo de ejecución de EKS para cuentas de miembros activas individuales

En esta sección se incluyen los pasos para configurar la Supervisión en tiempo de ejecución de EKS y administrar el agente de seguridad para cuentas de miembro activas individuales.

Según los [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (supervisión de todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>ENABLED</code>.

Enfoque preferido para administrar el agente de seguridad de GuardDuty

Pasos

GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.

También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y 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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de UnprocessedAccounts vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3.  Note Agregue siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor de STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'</pre>  Note También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de UnprocessedAccounts vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el par GuardDutyManaged -true. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] }]'</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración manual del agente de seguridad	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio <i>ID de detector</i>. Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita 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> Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente (API)

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas \(API\)](#).

Después de habilitar la Supervisión en tiempo de ejecución, asegúrese de instalar el agente de seguridad de GuardDuty mediante una configuración automática o una implementación manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Según los [Enfoques para administrar el agente de seguridad de GuardDuty en clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración del agente de seguridad a través de GuardDuty (supervisión de todos los clústeres de EKS)	1. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>. Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>ENABLED</code>. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. 2. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y 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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3.  Note Agregue siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor de STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de seguridad de GuardDuty se implementará en todos los clústeres de EKS de su cuenta. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED. Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	<pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'</pre>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations. En esta política, sustituya los detalles siguientes: • Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code>. • Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code>. • Sustituya <code>access-project</code> por <code>GuardDutyManaged</code>. • Sustituya <code>123456789012</code> por el ID de la Cuenta de AWS de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
	3. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>. Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>. GuardDuty administrará la implementación y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el par <code>GuardDutyManaged</code> <code>-true</code>. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita <code>EKS_RUNTIME_MONITORING</code> y se deshabilita <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>

Enfoque preferido para administrar el agente de seguridad de GuardDuty	Pasos
Administración manual del agente de seguridad	Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>. Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>. También puede utilizar el comando de la AWS CLI con su ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola https://console.aws.amazon.com/guardduty/ o ejecute la API ListDetectors. En el siguiente ejemplo se habilita <code>EKS_RUNTIME_MONITORING</code> y se deshabilita <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> Para administrar el agente de seguridad, consulte Administrar manualmente el agente de seguridad para el clúster de Amazon EKS.

Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución

Con el lanzamiento de la Supervisión de tiempo de ejecución de GuardDuty, la cobertura de detección de amenazas se ha ampliado a los contenedores de Amazon ECS y a las instancias de Amazon EC2. La experiencia de Supervisión en tiempo de ejecución de EKS se ha consolidado ahora en Supervisión en tiempo de ejecución. Puede habilitar la Supervisión en tiempo de ejecución y administrar agentes de seguridad de GuardDuty individuales para cada tipo de recurso (instancia de Amazon EC2, clúster de Amazon ECS y clúster de Amazon EKS) cuyo comportamiento en tiempo de ejecución desee supervisar.

GuardDuty ha consolidado la experiencia de la consola para la Supervisión en tiempo de ejecución de EKS en la Supervisión en tiempo de ejecución. GuardDuty recomienda [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#) y [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#).

Como parte de la migración a la Supervisión en tiempo de ejecución, asegúrese de [Desactivar la Supervisión en tiempo de ejecución de EKS](#). Esto es crucial porque, si en el futuro decide desactivar la Supervisión en tiempo de ejecución pero no desactiva la Supervisión en tiempo de ejecución de EKS, no dejará de incurrir en costos asociados al uso de esta última.

Para migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución

1. La consola de GuardDuty es compatible con la Supervisión en tiempo de ejecución de EKS como parte de la Supervisión en tiempo de ejecución.

Para comenzar a utilizar la Supervisión en tiempo de ejecución, puede [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#) de la organización y las cuentas.

Asegúrese de no desactivar la Supervisión en tiempo de ejecución de EKS antes de habilitar la Supervisión en tiempo de ejecución. Si desactiva la Supervisión en tiempo de ejecución de EKS, también se desactivará la administración del complemento de Amazon EKS. Siga los pasos que se indican a continuación en el mismo orden.

2. Asegúrese de cumplir todos los [Requisitos previos para habilitar la Supervisión en tiempo de ejecución](#).

3. Habilite la Supervisión en tiempo de ejecución. Para hacerlo, replique los mismos ajustes de configuración de la organización que utiliza para la Supervisión en tiempo de ejecución de EKS. Para obtener más información, consulte [Habilitación de la supervisión en tiempo de ejecución](#).
 - Si tiene una cuenta independiente, debe habilitar la Supervisión en tiempo de ejecución.

Si el agente de seguridad de GuardDuty ya está implementado, los ajustes correspondientes se replican automáticamente y no es necesario volver a configurarlos.
 - Si una organización utiliza la configuración de habilitación automática, asegúrese de replicar la misma configuración de habilitación automática para la Supervisión en tiempo de ejecución.
 - Si hay una organización con ajustes configurados para cuentas de miembro activas y existentes individualmente, asegúrese de habilitar la Supervisión en tiempo de ejecución y configurar el agente de seguridad de GuardDuty para estos miembros individualmente.
4. Una vez que se haya asegurado de que la configuración de la Supervisión en tiempo de ejecución y del agente de seguridad de GuardDuty es correcta, [desactive la Supervisión en tiempo de ejecución de EKS](#) mediante la API o el comando de la AWS CLI.
5. (Opcional) Si desea limpiar algún recurso asociado al agente de seguridad de GuardDuty, consulte [Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución](#).

Si desea continuar con el uso de la Supervisión en tiempo de ejecución de EKS sin activar la Supervisión en tiempo de ejecución, consulte [Supervisión en tiempo de ejecución de EKS en GuardDuty](#). En función de su caso de uso, elija los pasos para configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente o para varias cuentas de miembro.

Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS

Utilice las siguientes API o comandos de la AWS CLI para comprobar el estado de configuración existente de la Supervisión en tiempo de ejecución de EKS.

Para comprobar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS existente en la cuenta

- Ejecute [GetDetector](#) para comprobar el estado de configuración de una cuenta propia.
- Como alternativa, puede ejecutar el siguiente comando. Para ello, utilice la AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

Asegúrese de sustituir el ID de detector de la Cuenta de AWS y la región actual. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Para comprobar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS existente para la organización (solo como cuenta de administrador delegado de GuardDuty)

- Ejecute [DescribeOrganizationConfiguration](#) para comprobar el estado de configuración de la organización.

También puede ejecutar el siguiente comando mediante la AWS CLI:

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Asegúrese de sustituir el ID del detector por el ID del detector de la cuenta de administrador delegado de GuardDuty y la región por la región actual. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Desactivar la Supervisión en tiempo de ejecución de EKS después de migrar a la Supervisión en tiempo de ejecución

Una vez que se haya asegurado de que la configuración existente para la cuenta u organización se ha replicado en la Supervisión en tiempo de ejecución, podrá desactivar la Supervisión en tiempo de ejecución de EKS.

Para desactivar la Supervisión en tiempo de ejecución de EKS

- Para desactivar la Supervisión en tiempo de ejecución de EKS en una cuenta propia

Ejecute la API [UpdateDetector](#) con un *detector-id* regional propio.

También puede usar el siguiente comando de la AWS CLI: Sustituya *12abc34d567e8fa901bc2d34e56789f0* por su propio *detector-id* regional.


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

- Para desactivar la Supervisión en tiempo de ejecución de EKS para las cuentas de miembro de la organización

Ejecute la API [UpdateMemberDetectors](#) con el *detector-id* regional de la cuenta de administrador delegado de GuardDuty de la organización.

También puede usar el siguiente comando de la AWS CLI: Sustituya *12abc34d567e8fa901bc2d34e56789f0* por el *detector-id* regional de la cuenta de administrador delegado de GuardDuty de la organización y *111122223333* por el ID de la Cuenta de AWS de la cuenta de miembro para la que desea desactivar esta característica.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",  
"Status" : "DISABLED"}]'
```

- Para actualizar la configuración de habilitación automática de la Supervisión en tiempo de ejecución de EKS para la organización

Siga este paso únicamente si ha configurado la habilitación automática de la Supervisión en tiempo de ejecución de EKS para las cuentas nuevas (NEW) o para todas (ALL) las cuentas de miembro de la organización. Si ya ha establecido este ajuste como NONE, puede omitir este paso.

Note

Establecer la configuración de habilitación automática de la Supervisión en tiempo de ejecución de EKS en NONE significa que la Supervisión en tiempo de ejecución de EKS no se habilitará automáticamente para ninguna cuenta de miembro existente o cuando una nueva cuenta de miembro se una a la organización.

Ejecute la API [UpdateOrganizationConfiguration](#) con el *detector-id* regional de la cuenta de administrador delegado de GuardDuty de la organización.

También puede usar el siguiente comando de la AWS CLI: Sustituya *12abc34d567e8fa901bc2d34e56789f0* por el *detector-id* regional de la cuenta de

administrador delegado de GuardDuty de la organización. Sustituya el **EXISTING_VALUE** por la configuración actual para la habilitación automática de GuardDuty.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

Versiones del agente de seguridad de GuardDuty

GuardDuty lanza una versión actualizada del agente ocasionalmente. Cuando GuardDuty administra el agente automáticamente, está diseñado para actualizar el agente en su nombre. Si administra el agente manualmente, será responsable de actualizar la versión del agente para los tipos de recursos: instancias de Amazon EC2, clústeres de Amazon ECS y clústeres de Amazon EKS.

En las siguientes secciones se proporcionan las versiones del agente de seguridad de GuardDuty y las notas de la versión asociadas para todos los tipos de recursos admitidos.

Temas

- [Versiones del agente de seguridad de GuardDuty para instancias de Amazon EC2](#)
- [Versiones del agente de seguridad GuardDuty para AWS Fargate \(solo Amazon ECS\)](#)
- [Versiones del agente de seguridad GuardDuty para los recursos de Amazon EKS](#)
- [Recursos adicionales: próximos pasos](#)

Versiones del agente de seguridad de GuardDuty para instancias de Amazon EC2

En la siguiente tabla aparece el historial de versiones del agente de seguridad de GuardDuty para Amazon EC2.

Versión para distribuidores de SSM	Versión del agente	Notas de la versión	Fecha de disponibilidad
Versión 1.9.0	Versión 1.9.0	Mejoras y ajustes generales de rendimiento.	23 de octubre de 2025

Versión para distribuidores de SSM	Versión del agente	Notas de la versión	Fecha de disponibilidad
v1.8.0	v1.8.0	Mejoras y ajustes generales de rendimiento.	12 de agosto de 2025
v1.7.2	v1.7.1	Compatibilidad mejorada para la instalación de agentes locales para distribuciones de Linux basadas en RPM.	23 de julio de 2025
v1.7.1	1.7.1	Se agregó compatibilidad para Fedora 40 y Fedora 41. Para obtener una lista de todas las distribuciones de sistema operativo verificadas para los recursos de Amazon EC2, consulte Validar los requisitos de arquitectura . Mejoras y ajustes generales de rendimiento.	3 de junio de 2025

Versión para distribuidores de SSM	Versión del agente	Notas de la versión	Fecha de disponibilidad
v1.7.0	v1.7.0	Se agregó compatibilidad para las versiones 8.9 y 9.3 de Oracle Linux y para la versión 9.5 de Rocky Linux. Para obtener una lista de todas las distribuciones de sistema operativo verificadas para los recursos de Amazon EC2, consulte Validar los requisitos de arquitectura. Resolución de ID de contenedor mejorada. Mejoras y ajustes generales de rendimiento.	03 de abril de 2025
Versión 1.6.0	Versión 1.6.0	Mejoras y ajustes generales de rendimiento.	6 de febrero de 2025

Versión para distribuidores de SSM	Versión del agente	Notas de la versión	Fecha de disponibilidad
v1.5.0	v1.5.0	Se agregó compatibilidad para CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 y Ubuntu 24.04. Compatibilidad con instancias de ARM para resultados .../ MetadataDNSRebind . Mejoras y ajustes generales de rendimiento.	20 de noviembre de 2024
v1.3.1	v1.3.1	Compatibilidad con resolutores de DNS personalizados.	12 de septiembre de 2024
v1.3.0	v1.3.0	Mejoras y ajustes generales de rendimiento. Incluye compatibilidad para capturar señales de seguridad adicionales para futuros Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty.	19 de agosto de 2024

Versión para distribuidores de SSM	Versión del agente	Notas de la versión	Fecha de disponibilidad
v1.2.0	v1.2.0	Compatible con las distribuciones del sistema operativo Ubuntu 20.04, Ubuntu 22.04, Debian 11 y Debian 12. Compatible con los kernel 6.5 y 6.8 Mejoras y ajustes generales de rendimiento.	13 de junio de 2024
v1.1.0	v1.1.0	Admite la configuración automatizada del agente de GuardDuty en Runtime Monitoring para instancias de Amazon EC2 Admite nuevas señales de seguridad y resultados publicados con el anuncio de la disponibilidad general de Runtime Monitoring para instancias de EC2. Mejoras y ajustes generales de rendimiento.	26 de marzo de 2024

Versión para distribuidores de SSM	Versión del agente	Notas de la versión	Fecha de disponibilidad
v1.0.2	v1.0.2	Es compatible con las AMI más recientes de Amazon ECS.	2 de febrero de 2024
v1.0.1	v1.0.1	Las versiones del agente anteriores a la v1.0.2 no son compatibles con las AMI de Amazon ECS lanzadas después del 31 de enero de 2024. Mejoras y ajustes generales de rendimiento.	23 de enero de 2024
v1.0.0	v1.0.0	Versión inicial de la instalación RPM. Las versiones del agente anteriores a la v1.0.2 no son compatibles con las AMI de Amazon ECS lanzadas después del 31 de enero de 2024.	26 de noviembre de 2023

Versiones del agente de seguridad GuardDuty para AWS Fargate (solo Amazon ECS)

En la siguiente tabla aparece el historial de versiones del agente de seguridad de GuardDuty para Fargate (solo Amazon ECS).

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
Versión 1.9.0	x86_64 (AMD64): sha256:fd9acaa2326f180f0ed0c5a25d8ffc0a2d0498a6e900c34c68d4e973ea7fb26a8 Graviton (ARM64): sha256:0b04f8c28956684e752677bfd83dbc45afc8a43f7791fa44667b8078ba48a295	Mejoras de seguridad y ajustes generales de rendimiento.	28 de octubre de 2025
v1.8.0	x86_64 (AMD64): sha256:4425417f39e38b24c1be428bacad1dad53e0645530dcf4422436353bfe358e3a Graviton (ARM64): sha256:aff069418fd6825846f8	Mejoras y ajustes generales de rendimiento.	12 de agosto de 2025

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
	f575c4990 6a67c8a44 6d12d9ed0 d21ab95bd 0d05497b		
v1.7.0	x86_64 (AMD64): sha256:bf9197abdf853607e5fa392b4f97ccdd6ca56dd179be3ce8849e552d96582ac8 Graviton (ARM64): sha256:56c8683c948bcd82c0dbcebf755204365ac7285994693c11717bd45f86e279c2	Resolución de ID de contenedor mejorada. Mejoras y ajustes generales de rendimiento.	04 de abril de 2025

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
Versión 1.6.0	x86_64 (AMD64): sha256:c8 dea71d372 bc47b2f23 6f7a091b9 a9b06bc81 93c1cfe4c 9346eb50f 89258897 Graviton (ARM64): sha256:f4 032a566b9 0537646c2 a987bef42 eca1b4980 78ccc58a8 48603f877 971a8dbe	Mejoras y ajustes generales de rendimiento.	6 de febrero de 2025

Versión del agente	Imagen de contenedo r	Notas de la versión	Fecha de disponibi lidad
v1.5.0	x86_64 (AMD64): sha256:5e6fdc41f9eb748219d0b748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54 Graviton (ARM64): sha256:d56801ff6864d6014740103b70b1c38431851358d182613bede20fe21090e734	Compatibilidad con tareas de ARM para resultados .../ MetadataDNSRebind . Mejoras y ajustes generales de rendimiento.	14 de noviembre de 2024

Versión del agente	Imagen de contenedo r	Notas de la versión	Fecha de disponibi lidad
v1.4.1	x86_64 (AMD64): sha256:ef 36a11151e c2d3d7db2 2273bfb95 4750dee76 f0ac7bec3 7a7ba7e74 c3de1c78 Graviton (ARM64): sha256:a8 844544a59 d6b4cba98 f8e528b51 3ac2d9743 2f208e3ad 497cc16b3 31aa9faa	Endurecimiento de imágenes de contenedor. Mejoras y ajustes generales de rendimiento.	24 de octubre de 2024

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.3.1	x86_64 (AMD64): sha256:a6e2307d796e2875907bc4c1c69622c906f3192ddc42ef27b99e0a8f0979f3e0 Graviton (ARM64): sha256:ad1b6539d806edb504f17e6bcfb8b4026c5e822300afc31c0d23c6a08f9b99e9	Compatibilidad con resolvers de DNS personalizados.	11 de septiembre de 2024

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.3.0	x86_64 (AMD64): sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831 Graviton (ARM64): sha256:ff81a755d46681e409f55a95beeda9ebbcbf5336e1c0b1e6348af7c6518bdbb1	Mejoras y ajustes generales de rendimiento. Incluye compatibilidad para capturar señales de seguridad adicionales para futuros Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty de GuardDuty.	9 de agosto de 2024

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.2.0	x86_64 (AMD64): sha256:1d bad20ac2d c66d52d00 bb28dde42 81fe0d3c5 f261b1649 b247c2369 d9e26b93 Graviton (ARM64): sha256:91 930f8446f 5f95b93b8 ccb187739 92affa401 eb3f42da8 9d68077a5 6bafa6cd	Mejoras y ajustes generales de rendimiento.	31 de mayo de 2024

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.1.0	x86_64 (AMD64): sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657 Graviton (ARM64): sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7	Admite nuevas señales y resultados de seguridad. Mejoras y ajustes generales de rendimiento.	1 de mayo de 2024

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.0.1	x86_64 (AMD64): sha256:9f8cd438fb66f62d09bf c641286439f7ed5177988a314a6021ef4ff880642e68 Graviton (ARM64): sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	Mejoras y ajustes generales de rendimiento.	26 de enero de 2024

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.0.0	x86_64 (AMD64): sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton (ARM64): sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	Versión inicial del agente de seguridad de GuardDuty para AWS Fargate (solo Amazon ECS).	26 de noviembre de 2023

Versiones del agente de seguridad GuardDuty para los recursos de Amazon EKS

GuardDuty lanza una versión actualizada del agente ocasionalmente. Cuando GuardDuty administra el agente de manera automática, está diseñado para administrar las actualizaciones del agente en su nombre. Si administra el agente de manera manual, es responsable de actualizar la versión del agente para los clústeres de Amazon EC2.

Antes de actualizar el agente a una versión específica, añada el registro de imágenes de GuardDuty a los `allowed-container-registries` en el controlador de admisión. Para obtener más información, consulte [Repositorio de Amazon ECR que aloja el agente de GuardDuty](#).

En la siguiente tabla se muestra el historial de versiones de lanzamiento del [agente de GuardDuty del complemento de Amazon EKS](#).

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.11.0	x86_64 (AMD64): sha256:7c398fd50de5fe493c361aa7fe191e094ddfa000c65b449a9ed6a5cd53610e7 Graviton (ARM64): sha256:98a547b47d4770f45e75eb9730c807d9265722ca2f391e0aa5cb19e487ab455f	Se agregó compatibilidad para las distribuciones de sistemas operativos Fedora 40 y Fedora 41. Para obtener más información, consulte Validación de los requisitos de arquitectura (para EKS). Mejoras de seguridad y ajustes generales de rendimiento.	29 de agosto de 2025	–
v1.10.0	x86_64 (AMD64): sha256:6dcbe5b055e1ef0af903071ede0b08f755ad5b7e9774a67df5399efd aa1f3d7d	Resolución de ID de contenedor mejorada. Mejoras y ajustes generales de rendimiento.	04 de abril de 2025	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
	Graviton (ARM64): sha256:f0 536882268 9610a4bab 543abf93d 3e070b1b5 59e62a2e6 7d82dfa98 37600f72			
Versión 1.9.0	x86_64 (AMD64): sha256:51 c5789ef65 70f9bec87 9ac48a8f4 769718cbc 31e454300 32569917e 219af63f Graviton (ARM64): sha256:9c 2f74e7ea0 827b7e422 ae4c91fff c6c2bc41a 1cdb96c71 91d05259d 337154e1	Mejoras y ajustes generales de rendimiento.	2 de marzo de 2025	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.8.1	x86_64 (AMD64): sha256:f2ce8cf89db e17e3388c ecb350535 44dadf21a f7770545f 8d4b50384 076aff47 Graviton (ARM64): sha256:30f586e4b69 4e704bcaf adfa9081a b0aef3cf bcde39743 a0f1e24f7 7d79627f	Se agregó compatibilidad para CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 y Ubuntu 24.04. Compatibilidad con instancias de ARM para resultados .../MetadataDNSRebind . Mejoras y ajustes generales de rendimiento.	23 de noviembre de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.7.1	x86_64 (AMD64): sha256:b8b86b5d0872c8b67fecf64ec3d172666360545435a1752447d510951a7fd749 Graviton (ARM64): sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9	Mejoras y ajustes generales de rendimiento. Incluye compatibilidad para capturar señales de seguridad adicionales para futuros Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty . Compatibilidad con resolutores de DNS personalizados.	13 de septiembre de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.7.0	x86_64 (AMD64): sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffc7e68554a423d610cea8c7e8f2185ec Graviton (ARM64): sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a	Mejoras y ajustes generales de rendimiento. Incluye compatibilidad para capturar señales de seguridad adicionales para futuros Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty.	17 de agosto de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.6.1	x86_64 (AMD64): sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bd b07c3ab1 Graviton (ARM64): sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019	Mejoras y ajustes generales de rendimiento.	14 de mayo de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
Versión 1.6.0	x86_64 (AMD64): sha256:7d abcbec30d 8b0536767 52fbc19e8 9f77272d9 a6a53cc93 731f58721 80ef9010 Graviton (ARM64): sha256:97 10f53afcc df4f22b26 5a1a6fc27 f1469403a f1f7d5d08 c4869a726 9cdd2650	• Admite la configuración automatizada del agente de GuardDuty para recursos EKS/EC2. • Admite nuevas señales y resultados de seguridad. Para obtener más información, consulte Tipos de eventos de tiempo de ejecución recopilados que utiliza GuardDuty y Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty. • Mejoras y ajustes generales de rendimiento.	29 de abril de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.5.0	x86_64 (AMD64): sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Graviton (ARM64): sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	- Mejoras y ajustes generales de rendimiento. - Mejoras de seguridad, incluidos nuevos tipos de eventos en Tipos de eventos de tiempo de ejecución recopilados. - Mejoras de rendimiento en relación con el uso de la CPU.	7 de marzo de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.4.1	x86_64 (AMD64): sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c Graviton (ARM64): sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dff e0792c9e6d0778b40	Mejoras y ajustes generales de rendimiento.	16 de enero de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.4.0	x86_64 (AMD64): sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f Graviton (ARM64): sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e	El punto de montaje del manifiesto admite una mejor recopilación de datos Configuración de AppArmor en el manifiesto Argumento recopilar de la línea de comandos Mejoras y ajustes generales de rendimiento	21 de diciembre de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.3.1	x86_64 (AMD64): sha256:55 578fcb7b7 3097ade5c 8404390ef 16cf76a7b 568490aba ae01ac759 92b3ea29 Graviton (ARM64): sha256:e3 ce8d66ac2 121f8d476 eb58f8bc5 0ab513366 47615eb7c f514c2142 1cb818fd	Actualizaciones y revisiones de seguridad importantes.	23 de octubre de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.3.0	x86_64 (AMD64): sha256:6d ace2337df bb7609811 be89fb4b2 3ae0b865f 1027ad78f be69530bf bd46c694 Graviton (ARM64): sha256:49 28a7c6ef4 0e77c8ec9 5841323bb 9a110db31 f12c0ee7a b965e08b4 3efd01bb	Compatible con la plataforma Ubuntu Compatible con la versión 1.28 de Kubernetes Mejoras generales de rendimiento y de estabilidad.	5 de octubre de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.2.0	x86_64 (AMD64): sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3 Graviton (ARM64): sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa	Además de las instancias basadas en AMD64, la versión 1.2.0 ahora también admite las instancias basadas en ARM64. Se ha agregado compatibilidad con Bottlerocket y se ha verificado. Compatible con la versión 1.27 de Kubernetes Mejoras generales de rendimiento y de estabilidad.	16 de junio de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Finalización del soporte estándar ¹
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	Además de las Versiones de Kubernetes compatibles con el agente de seguridad de GuardDuty , esta versión del agente también es compatible con la versión 1.26 de Kubernetes. Mejoras generales de rendimiento y de estabilidad.	2 de mayo de 2023	14 de mayo de 2024
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Versión inicial del agente del complemento de Amazon EKS.	30 de marzo de 2023	14 de mayo de 2024

¹ Para obtener información sobre cómo actualizar la versión actual del agente que está a punto de finalizar su soporte estándar, consulte [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#).

Recursos adicionales: próximos pasos

Para obtener más información sobre los próximos pasos, consulte los siguientes temas:

- [Requisitos previos para habilitar la Supervisión en tiempo de ejecución](#): con las nuevas versiones de los agentes, es posible que se actualice la sección de requisitos previos. Verifique y valide que sus recursos cumplen los requisitos previos más recientes.
- [Administrar los agentes de seguridad de GuardDuty](#): si administra el agente manualmente, es responsable de administrar las actualizaciones de la versión del agente que se ejecuta en sus recursos. Según el tipo de recurso (Amazon EKS o Amazon EC2-Amazon ECS), lleve a cabo los pasos para actualizar el agente de seguridad. Asegúrese también de validar la [configuración de punto de conexión de VPC](#).
- [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#): una vez que haya actualizado el agente de seguridad, podrá evaluar la cobertura de tiempo de ejecución de su recurso. Si hay algún problema de cobertura, siga los pasos de solución de problemas asociados.

Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución

Esta sección se aplica a la Cuenta de AWS si opta por desactivar la Supervisión en tiempo de ejecución, o únicamente la configuración automatizada del agente de GuardDuty para un tipo de recurso.

Desactivar la configuración automatizada del agente de GuardDuty

GuardDuty no elimina el agente de seguridad implementado en el recurso. Sin embargo, GuardDuty dejará de administrar las actualizaciones del agente de seguridad.

GuardDuty no dejará de recibir los eventos en tiempo de ejecución del tipo de recurso. Para evitar que las estadísticas de uso se vean afectadas, asegúrese de eliminar el agente de seguridad de GuardDuty del recurso.

Tanto si una Cuenta de AWS utiliza un punto de conexión de VPC compartida como si no, GuardDuty no elimina el punto de conexión de VPC. Si es necesario, tendrá que eliminar el punto de conexión de VPC manualmente.

Desactivar la Supervisión en tiempo de ejecución y la Supervisión en tiempo de ejecución de EKS

Esta sección se aplica en los siguientes casos:

- Nunca habilitó la Supervisión en tiempo de ejecución de EKS por separado y ahora desactivó la Supervisión en tiempo de ejecución.
- Va a desactivar tanto la Supervisión en tiempo de ejecución como la Supervisión en tiempo de ejecución de EKS. Si no está seguro del estado de configuración de la Supervisión en tiempo de ejecución de EKS, consulte [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#).

Desactivar la Supervisión en tiempo de ejecución sin desactivar la Supervisión en tiempo de ejecución de EKS

En este caso, en algún momento, habilitó la Supervisión en tiempo de ejecución de EKS y, posteriormente, también habilitó la Supervisión en tiempo de ejecución sin desactivar la Supervisión en tiempo de ejecución de EKS.

Ahora, al desactivar la Supervisión en tiempo de ejecución, también deberá desactivar la Supervisión en tiempo de ejecución de EKS; de lo contrario, no dejará de incurrir en gastos por el uso de la Supervisión en tiempo de ejecución de EKS.

Si los casos mencionados anteriormente se aplican a su situación, entonces GuardDuty tomará las siguientes acciones en su cuenta:

- GuardDuty elimina el punto de conexión de VPC que tiene la etiqueta `GuardDutyManaged:true`. Esta es la VPC que GuardDuty había creado para administrar el agente de seguridad automatizado.
- GuardDuty elimina el grupo de seguridad etiquetado como `GuardDutyManaged:true`.
- En el caso de una VPC compartida que ha sido utilizada por al menos una cuenta participante, GuardDuty no elimina ni el punto de conexión de VPC ni el grupo de seguridad asociado al recurso de VPC compartida.
- En el caso de un recurso de Amazon EKS, GuardDuty elimina el agente de seguridad. Esto es independiente de si se administra manualmente o a través de GuardDuty.

En el caso de un recurso de Amazon ECS, dado que las tareas de ECS son inmutables, GuardDuty no puede desinstalar el agente de seguridad de ese recurso. Esto es independiente de cómo se administra el agente de seguridad (manual o automáticamente a través de GuardDuty). Después de desactivar la Supervisión en tiempo de ejecución, GuardDuty no

asociará un contenedor sidecar cuando se comience a ejecutar una nueva tarea de ECS. Para obtener información sobre cómo trabajar con tareas Fargate-ECS, consulte [Cómo funciona la supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#).

En el caso de un recurso de Amazon EC2, GuardDuty desinstala el agente de seguridad de todas las instancias de Amazon EC2 administradas por Systems Manager (SSM) únicamente cuando se cumplen las siguientes condiciones:

- El recurso no está etiquetado con la etiqueta de exclusión `GuardDutyManaged:false`.
- GuardDuty debe tener permisos para acceder a las etiquetas de los metadatos de instancia. Para este recurso de EC2, el Acceso a etiquetas en metadatos de instancia está establecido en Permitir.

Al dejar de administrar manualmente el agente de seguridad

Independientemente del enfoque que utilice para implementar y administrar el agente de seguridad de GuardDuty, para dejar de supervisar los eventos en tiempo de ejecución en el recurso, debe eliminar el agente de seguridad de GuardDuty. Cuando desee dejar de supervisar los eventos en tiempo de ejecución de un tipo de recurso en una cuenta, también puede eliminar el punto de conexión de Amazon VPC.

Desinstalar manualmente el agente de seguridad para los recursos de Amazon EC2

En esta sección se describen métodos para desinstalar el agente de seguridad de GuardDuty de los recursos de Amazon EC2. Si administra el agente de seguridad manualmente, es responsable de eliminar el agente de los recursos. GuardDuty no tomará ninguna acción respecto a los recursos que administra.

Si creó un punto de conexión de Amazon VPC manualmente, después de desinstalar el agente de seguridad en todos los tipos de recursos supervisados de la cuenta, podrá optar por eliminar el punto de conexión de VPC. Se trata de un paso separado. Para obtener más información, consulte [To delete a VPC endpoint](#).

En función de cómo haya instalado el agente de seguridad en el recurso, elija uno de los siguientes métodos para desinstalarlo.

Temas

- [Método 1: mediante el Comando de ejecución](#)

- [Método 2: mediante administradores de paquetes de Linux](#)

Método 1: mediante el Comando de ejecución

Si instaló el agente de seguridad con [Método 1: usar AWS Systems Manager](#), siga estos pasos para desinstalarlo:

Para desinstalar el agente de seguridad de GuardDuty

1. Para desinstalar el agente de seguridad GuardDuty, puede seguir los pasos especificados en [Comando de ejecución de AWS Systems Manager](#) en la Guía del usuario de AWS Systems Manager. Use la acción Desinstalar en los parámetros para desinstalar el agente de seguridad de GuardDuty.

En la sección Destinos, asegúrese de que el impacto se produce únicamente en las instancias de Amazon EC2 de las que desea desinstalar el agente de seguridad.

Utilice el siguiente documento de GuardDuty y distribuidor:

- Nombre del documento: AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
 - Distributor: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. Después de proporcionar todos los detalles, cuando elija Ejecutar, se eliminará el agente de seguridad que implementó en las instancias de Amazon EC2 de destino.

Para eliminar la configuración del punto de conexión de Amazon VPC, debe desactivar tanto la Supervisión en tiempo de ejecución como la Supervisión en tiempo de ejecución de Amazon EKS.

3. Si también desea eliminar el punto de conexión de VPC asociado a este agente de seguridad, consulte [To delete a VPC endpoint](#).

Método 2: mediante administradores de paquetes de Linux

Si instaló el agente de seguridad con [Método 2: utilizar administradores de paquetes de Linux](#), siga estos pasos para desinstalarlo:

Para desinstalar el agente de seguridad de GuardDuty

1. Conecte con la instancia. Para conocer los pasos necesarios, consulte [Establecer conexión con la instancia de Linux mediante un cliente SSH](#) en la Guía del usuario de Amazon EC2.
2. Comando para la desinstalación

El siguiente comando desinstalará el agente de seguridad de GuardDuty de la instancia de Amazon EC2 con la que se haya establecido la conexión:

- Para RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Para Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Después de ejecutar el comando, también puede comprobar los registros asociados a este.

3. Si también desea eliminar el punto de conexión de VPC asociado a este agente de seguridad, consulte [To delete a VPC endpoint](#).

Limpiar los recursos de los agentes de seguridad

En esta sección se explica cómo se pueden limpiar los recursos de AWS asociados al agente de seguridad. Como se indica en [Desactivar, desinstalar y limpiar recursos](#), GuardDuty no eliminará ni quitará todos los recursos de los agentes de seguridad. En la siguiente sección se ofrecen instrucciones sobre cómo eliminar los recursos del agente de seguridad.

Eliminación del punto de conexión de VPC de Amazon

Si administra el agente de seguridad manualmente, es posible que haya creado un punto de conexión de Amazon VPC manualmente. Después de desinstalar el agente de seguridad para todos los recursos supervisados en la cuenta, podrá optar por eliminar este punto de conexión de VPC.

En la siguiente lista se presentan distintos casos en los que se puede utilizar una VPC compartida en lugar de no utilizarla.

- Sin una VPC compartida: Cuando ya no desee supervisar un recurso en una cuenta, considere la posibilidad de eliminar el punto de conexión de Amazon VPC.
- Cuando una cuenta de propietario de una VPC compartida elimina el recurso de la VPC compartida que aún se utilizaba, la cobertura de la Supervisión en tiempo de ejecución (y, cuando corresponda, de la Supervisión en tiempo de ejecución de EKS) para los recursos de la cuenta de propietario de la VPC compartida y de la cuenta participante podría pasar a estar en mal estado. Para obtener información sobre el estado de la cobertura, consulte [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Para eliminar un punto de conexión de VPC, consulte [Eliminar un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink.

Para eliminar el grupo de seguridad

- Sin una VPC compartida: cuando ya no desee supervisar un tipo de recurso en una cuenta, considere la opción de eliminar el grupo de seguridad asociado a la Amazon VPC.
- Con una VPC compartida: cuando la cuenta de propietario de la VPC compartida elimina el grupo de seguridad, cualquier cuenta de participante que actualmente utilice el grupo de seguridad asociado a la VPC compartida, el estado de cobertura de la Supervisión en tiempo de ejecución para los recursos de la cuenta de propietario de la VPC compartida y la cuenta de participante podrían quedar en mal estado. Para obtener más información, consulte [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Para obtener información sobre los pasos, consulte [Eliminar un grupo de seguridad de Amazon EC2](#) en la Guía del usuario de Amazon EC2.

Para eliminar el agente de seguridad de GuardDuty de un clúster de EKS

Para eliminar del clúster de EKS el agente de seguridad que ya no desea supervisar, consulte [Eliminar del clúster un complemento de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Al eliminar el agente del complemento de EKS, no se elimina el espacio de nombres amazon-guardduty del clúster de EKS. Para eliminar el espacio de nombres amazon-guardduty, consulte [Deleting a namespace](#).

Para eliminar el espacio de nombres **amazon-guardduty** (clúster de EKS)

Al desactivar la configuración automatizada del agente, no se elimina automáticamente del clúster de EKS el espacio de nombres amazon-guardduty. Para eliminar el espacio de nombres amazon-guardduty, consulte [Deleting a namespace](#).

Protección contra malware de GuardDuty para EC2

La protección contra malware para EC2 ayuda a detectar la posible presencia de malware mediante el análisis de los [volúmenes de Amazon Elastic Block Store \(Amazon EBS\)](#) que se asocian a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y a las cargas de trabajo de contenedores que se ejecutan en Amazon EC2. La protección contra malware para EC2 ofrece opciones de análisis en las que puede decidir si desea incluir o excluir instancias específicas de Amazon EC2 en el momento del análisis. También ofrece la opción de retener las instantáneas de los volúmenes de Amazon EBS adjuntos a las instancias o cargas de trabajo de contenedores de Amazon EC2 en sus cuentas de GuardDuty. Las instantáneas se retienen solo cuando se encuentra malware y se generan resultados de la protección contra malware para EC2.

La protección contra malware para EC2 se diseñó de forma que no afecte al rendimiento de los recursos. Para obtener información sobre cómo funciona la protección contra malware para EC2 en GuardDuty, consulte [Cómo GuardDuty analiza los volúmenes de EBS para detectar malware](#). Para obtener información sobre la disponibilidad de la protección contra malware para EC2 en diferentes Regiones de AWS, consulte [Regiones y puntos de conexión](#).

Notas

Malware Protection for EC2 es compatible con análisis de malware en instancias administradas para modo automático de Amazon EKS.

Malware Protection for EC2 no es compatible con análisis de malware para cargas de trabajo AWS Fargate que se ejecutan en Amazon EKS ni en Amazon ECS.

Para obtener más información sobre estas características de Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

Temas

- [Comparación del análisis de malware iniciado por GuardDuty y el análisis de malware bajo demanda](#)
- [Cómo GuardDuty analiza los volúmenes de EBS para detectar malware](#)
- [Volúmenes de Amazon EBS compatibles con el análisis de malware](#)
- [Configure la retención de instantáneas y la cobertura de análisis de EC2](#)
- [Análisis de malware iniciado por GuardDuty](#)
- [Análisis de malware bajo demanda en GuardDuty](#)

- [Supervisión de los estados y resultados de los análisis en Malware Protection for EC2](#)
- [Cuentas de servicio de GuardDuty por Región de AWS](#)
- [Cuotas en la protección contra malware de EC2](#)

Comparación del análisis de malware iniciado por GuardDuty y el análisis de malware bajo demanda

La protección contra malware para EC2 ofrece dos tipos de análisis para detectar posibles actividades maliciosas en las instancias y cargas de trabajo de contenedores de Amazon EC2: el análisis de malware iniciado por GuardDuty y el análisis de malware bajo demanda. En la siguiente tabla, se muestra la comparación entre ambos tipos de análisis.

Factor	Análisis de malware iniciado por GuardDuty	Análisis de malware bajo demanda
Cómo se invoca el análisis	Tras activar el análisis de malware iniciado por GuardDuty, siempre que GuardDuty arroje un resultado que indique la posible presencia de malware en una instancia o carga de trabajo de un contenedor de Amazon EC2, GuardDuty inicia automáticamente un análisis de malware sin agente en los volúmenes de Amazon EBS adjuntos al recurso potencialmente afectado. Para obtener más información, consulte Análisis de malware iniciado por GuardDuty .	Para iniciar un análisis de malware bajo demanda, puede proporcionar el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2. Puede iniciar un análisis de malware bajo demanda incluso cuando GuardDuty no devuelva un resultado respecto a su recurso. Para obtener más información, consulte Análisis de malware bajo demanda en GuardDuty .
Se necesita configuración	Para utilizar el análisis de malware iniciado por GuardDuty, debe habilitarlo	La cuenta debe tener GuardDuty habilitado. Para utilizar el análisis de malware

Factor	Análisis de malware iniciado por GuardDuty	Análisis de malware bajo demanda
	en su cuenta. Para administrar varias cuentas mediante AWS Organizations o el método basado en invitaciones, consulte Habilitar el análisis de malware iniciado por GuardDuty en entornos de varias cuentas. Para habilitar el análisis de malware iniciado por GuardDuty en una cuenta propia, consulte Habilitar el análisis de malware iniciado por GuardDuty para una cuenta independiente.	bajo demanda, no se requiere ninguna configuración a nivel de característica.
Tiempo de espera para iniciar un nuevo análisis	Cada vez que GuardDuty genera uno de los Resultados que invocan un análisis de malware iniciado por GuardDuty, se inicia automáticamente un análisis de malware solo una vez cada 24 horas.	Puede iniciar un análisis de malware bajo demanda en el mismo recurso en cualquier momento después de 1 hora tras la hora de inicio del análisis anterior.

Factor	Análisis de malware iniciado por GuardDuty	Análisis de malware bajo demanda
Disponibilidad del periodo de prueba gratuito de 30 días ¹	Al habilitar el análisis de malware iniciado por GuardDuty por primera vez en la cuenta, puede utilizar un periodo de prueba gratuito de 30 días. Para obtener más información, consulte Prueba gratuita de 30 días en el análisis de malware iniciado por GuardDuty.	No se ofrece un período de prueba gratuito para el análisis de malware bajo demanda en cuentas nuevas o existentes de GuardDuty.
Opciones de análisis ²	Tras configurar el análisis de malware iniciado por GuardDuty, la protección contra malware para EC2 permite incluir o excluir recursos específicos de Amazon EC2 mediante etiquetas. La Protección contra malware para EC2 no iniciará un análisis automático de los recursos que decida excluir de este. Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario.	Dado que usted proporciona el ARN del recurso para iniciar manualmente un análisis de malware bajo demanda, el uso de Opciones de análisis con etiquetas definidas por el usuario no resulta aplicable.

¹ Incurrirá en costos de uso al crear y retener las instantáneas de los volúmenes de EBS. Para obtener más información sobre cómo configurar la cuenta para retener instantáneas, consulte [Retención de instantáneas](#).

²Tanto el análisis de malware iniciado por GuardDuty como el análisis bajo demanda permiten utilizar una etiqueta global para excluir recursos de Amazon EC2 de los análisis de malware. Para obtener más información, consulte [Etiqueta GuardDutyExcluded global](#).

Cómo GuardDuty analiza los volúmenes de EBS para detectar malware

En esta sección, se explica cómo la protección contra malware para EC2, que incluye tanto el análisis de malware iniciado por GuardDuty como el análisis de malware bajo demanda, analiza los volúmenes de Amazon EBS asociados a las instancias y cargas de trabajo de contenedores de Amazon EC2. Antes de continuar, tenga en cuenta las siguientes personalizaciones:

- **Opciones de análisis:** la Protección contra malware para EC2 ofrece la posibilidad de especificar etiquetas para incluir o excluir las instancias de Amazon EC2 y los volúmenes de Amazon EBS del proceso de análisis. Solo el análisis de malware iniciado por GuardDuty admite opciones de análisis con etiquetas definidas por el usuario. Tanto el análisis de malware iniciado por GuardDuty como el análisis de malware bajo demanda admiten la etiqueta global GuardDutyExcluded. Para obtener más información, consulte [Opciones de análisis con etiquetas definidas por el usuario](#).
- **Retención de instantáneas:** la protección contra malware para EC2 ofrece una opción para retener las instantáneas de los volúmenes de Amazon EBS en la cuenta de AWS. Por defecto, esta opción está desactivada. Puede optar por la retención de instantáneas tanto para los análisis de malware iniciados por GuardDuty como para los análisis bajo demanda. Para obtener más información, consulte [Retención de instantáneas](#).

Si GuardDuty genera uno o más [Resultados que invocan un análisis de malware iniciado por GuardDuty](#), será motivo para que GuardDuty inicie un análisis de malware. Si las opciones de análisis no excluyen esta instancia, GuardDuty iniciará el análisis.

Para iniciar un análisis de malware bajo demanda en los volúmenes de Amazon EBS asociados a una instancia de Amazon EC2, proporcione el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2.

Como respuesta al inicio de un análisis de malware bajo demanda o un análisis automático iniciado por GuardDuty, este servicio crea instantáneas de los volúmenes de EBS relevantes asociados con el recurso potencialmente afectado y las comparte con la [Cuentas de servicio de GuardDuty](#). Cuando GuardDuty crea instantáneas de los volúmenes de EBS, agrega una etiqueta predeterminada llamada GuardDutyScanId. Esta etiqueta ayuda a GuardDuty a acceder a la instantánea.

Asegúrese de no quitar esta etiqueta. A partir de estas instantáneas, GuardDuty crea una réplica cifrada del volumen de EBS en la cuenta de servicio.

Una vez finalizado el análisis, GuardDuty elimina las réplicas cifradas y las instantáneas de los volúmenes de EBS. La configuración de retención de instantáneas está desactivada de manera predeterminada. Sin embargo, las instantáneas se conservan si el [bloqueo de instantáneas de Amazon EBS](#) está habilitado para ellas, independientemente de los resultados y la configuración del análisis. GuardDuty no puede modificar la configuración de bloqueo de instantáneas de Amazon EBS.

En la siguiente lista se describe el comportamiento de retención de las instantáneas, independientemente del bloqueo de instantáneas de EBS:

La retención de instantáneas está activada:

- Cuando se encuentra malware, GuardDuty retiene las instantáneas en su Cuenta de AWS.
- Cuando no se encuentra ningún malware, GuardDuty no conserva las instantáneas a menos que estén bloqueadas.

La retención de instantáneas está desactivada (de manera predeterminada):

- Tanto si se encuentra malware como si no, las instantáneas no se retienen.
- GuardDuty no puede eliminar las instantáneas bloqueadas de Amazon EBS.

GuardDuty retendrá cada de réplica de volumen de EBS en la cuenta de servicio durante un máximo de 55 horas. Si se produce una interrupción del servicio o un error con la réplica de un volumen de EBS y su análisis de malware, GuardDuty retendrá dicho volumen de EBS durante un máximo de siete días. El periodo prolongado de retención del volumen sirve para clasificar y solucionar la interrupción o el error. La protección contra malware de GuardDuty para EC2 eliminará las réplicas de los volúmenes de EBS de la cuenta de servicio una vez que se solucione la interrupción o el error, o una vez que haya transcurrido el periodo de retención prolongado.

Para obtener información sobre la metodología de detección de malware de GuardDuty y los motores de análisis que utiliza, consulte [Motor de análisis de detección de malware de GuardDuty](#).

Volúmenes de Amazon EBS compatibles con el análisis de malware

En todas aquellas Regiones de AWS en las que GuardDuty admite la característica de protección contra malware para EC2, puede analizar los volúmenes de Amazon EBS cifrados o sin cifrar.

Puede tener volúmenes de Amazon EBS cifrados con una [Clave administrada de AWS](#) o [una clave administrada por el cliente](#). Actualmente, algunas de las regiones en las que la protección contra malware para EC2 se encuentra disponible admiten ambas formas de cifrar los volúmenes de Amazon EBS, mientras que otras solo admiten la clave administrada por el cliente. Para obtener información acerca de las regiones de admitidas, consulte [Cuentas de servicio de GuardDuty por Región de AWS](#). Para obtener información sobre las regiones en las que GuardDuty está disponible pero no está disponible Malware Protection for EC2, consulte [Disponibilidad de características específicas por región](#).

En la siguiente lista se describe la clave que GuardDuty utiliza tanto si los volúmenes de Amazon EBS están cifrados como si no:

- Volúmenes de Amazon EBS sin cifrar o cifrados con Clave administrada de AWS: GuardDuty utiliza su propia clave para cifrar las réplicas de volúmenes de Amazon EBS.

Si la región no admite el análisis de volúmenes de Amazon EBS cifrados con el [cifrado de Amazon EBS de forma predeterminada](#), deberá modificar la clave predeterminada de modo que sea una clave administrada por el cliente. Esto ayudará a GuardDuty a acceder a estos volúmenes de EBS. Al modificar la clave, incluso los futuros volúmenes de EBS se crearán con la clave actualizada de modo que GuardDuty pueda admitir análisis de malware. Para conocer los pasos a seguir para modificar la clave predeterminada, consulte [Modificar el ID de clave de AWS KMS predeterminada de un volumen de Amazon EBS](#) en la siguiente sección.

- Volúmenes de Amazon EBS cifrados con clave administrada por el cliente: GuardDuty utiliza la misma clave para cifrar el volumen de EBS de réplica. Para obtener información sobre qué políticas relacionadas con el cifrado de AWS KMS son admitidas, consulte [Permisos de rol vinculado al servicio para Malware Protection for EC2](#).

Modificar el ID de clave de AWS KMS predeterminada de un volumen de Amazon EBS

Al crear un volumen de Amazon EBS mediante el [cifrado de Amazon EBS](#) y no especificar el ID de clave de AWS KMS, el volumen de Amazon EBS se cifra con una [clave de cifrado predeterminada](#). Al habilitar el cifrado de forma predeterminada, Amazon EBS cifrará automáticamente los nuevos volúmenes e instantáneas por medio de la clave de KMS predeterminada para el cifrado de Amazon EBS.

Puede modificar la clave de cifrado predeterminada y utilizar una clave administrada por el cliente para el cifrado de Amazon EBS. Esto ayudará a GuardDuty a acceder a estos volúmenes de Amazon EBS. Para modificar la ID de clave predeterminada de EBS, agregue el siguiente permiso necesario a su política de IAM: `ec2:modifyEbsDefaultKmsKeyId`. Cualquier volumen de Amazon EBS recién creado que elija cifrar, pero no especifique un ID de clave de KMS asociada, utilizará el ID de clave predeterminada. Utilice uno de los siguientes métodos para actualizar el ID de clave predeterminada de EBS:

Modificación de la ID de clave de KMS predeterminada de un volumen de Amazon EBS

Realice una de las siguientes acciones:

- Uso de una API: puede utilizar la API [ModifyEbsDefaultKmsKeyId](#). Para obtener información sobre cómo puede ver el estado de cifrado del volumen, consulte [Crear volumen de Amazon EBS](#).
- Uso de comandos de la AWS CLI: el siguiente ejemplo modifica la ID de clave de KMS predeterminada que cifrará los volúmenes de Amazon EBS si no proporciona una ID de clave de KMS. Asegúrese de sustituir la región por la Región de AWS de su ID de clave de KMS.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

El comando anterior generará un resultado similar al siguiente:

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Para obtener más información, consulte [modify-ebs-default-kms-key-id](#).

Configure la retención de instantáneas y la cobertura de análisis de EC2

En esta sección, se explica cómo personalizar las opciones de análisis de malware para las instancias de Amazon EC2. Estas personalizaciones se aplican tanto a los análisis de malware bajo demanda como a los iniciados por GuardDuty. Puede hacer lo siguiente:

- Habilitar la retención de instantáneas: si se habilita antes de un análisis, GuardDuty conservará la instantánea de Amazon EBS que GuardDuty detectó como maliciosa.

- Elija qué instancias de Amazon EC2 desea analizar: utilice etiquetas para incluir o excluir instancias de Amazon EC2 específicas de los análisis de malware.

Retención de instantáneas

GuardDuty le ofrece la opción de retener las instantáneas de sus volúmenes de EBS en su cuenta de AWS. La configuración de retención de instantáneas está desactivada de manera predeterminada. Las instantáneas solo se retendrán si ha activado esta configuración antes de que se inicie el análisis.

Cuando se inicia el análisis, GuardDuty genera las réplicas de los volúmenes de EBS en función de las instantáneas de sus volúmenes de EBS. Cuando se complete el análisis y se haya activado la configuración de conservación de instantáneas en su cuenta, las instantáneas de sus volúmenes de EBS solo se retendrán cuando se detecte malware y se genere [Tipos de resultados de la protección contra malware para EC2](#). Si no se encuentra ningún malware, GuardDuty elimina automáticamente las instantáneas de los volúmenes de EBS, a menos que se haya activado el [bloqueo de instantáneas de Amazon EBS](#) en las instantáneas creadas.

Costo de uso de instantáneas

Durante el análisis de malware, a medida que GuardDuty crea las instantáneas de los volúmenes de Amazon EBS, este paso conlleva un costo de uso. Si activa la configuración de retención de instantáneas en su cuenta, cuando se detecte malware y se conserven las instantáneas, incurrirá en costos de uso por el mismo. Para obtener información sobre el costo de las instantáneas y su retención, consulte [Precios de Amazon EBS](#).

Como cuenta de administrador delegado de GuardDuty, solo puede realizar esta actualización en nombre de las cuentas de miembro de la organización. Sin embargo, si una cuenta de miembro se [administra mediante el método de invitación](#), esta podrá realizar este cambio por su cuenta. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija su método de acceso preferido para activar la configuración de retención de instantáneas.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, en Planes de protección, elija Protección contra malware para EC2.

3. Elija Configuración general en la sección inferior de la consola. Para retener las instantáneas, active Retención de instantáneas.

API/CLI

Ejecute [UpdateMalwareScanSettings](#) para actualizar la configuración actual de retención de instantáneas.

Como alternativa, puede ejecutar el siguiente comando de la AWS CLI para retener automáticamente las instantáneas cuando la protección contra malware de GuardDuty para EC2 genere resultados.

Asegúrese de sustituir el *detector-id* por su propio detectorId válido.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Si desea desactivar la retención de instantáneas, sustituya RETENTION_WITH_FINDING por NO_RETENTION.

Opciones de análisis con etiquetas definidas por el usuario

Al utilizar el análisis de malware iniciado por GuardDuty, también puede especificar etiquetas para incluir o excluir las instancias de Amazon EC2 y los volúmenes de Amazon EBS del proceso de análisis y detección de amenazas. Para personalizar cada análisis de malware iniciado por GuardDuty, puede editar las etiquetas de la lista de etiquetas de inclusión o exclusión. Cada lista puede incluir hasta 50 etiquetas.

Si aún no tiene etiquetas definidas por el usuario asociadas a los recursos de EC2, consulte [Etiquetar los recursos de Amazon EC2](#) en la Guía del usuario de Amazon EC2.

 Note

El análisis de malware bajo demanda no admite opciones de análisis con etiquetas definidas por el usuario. Es compatible con [Etiqueta GuardDutyExcluded global](#).

Exclusión de las instancias de EC2 del análisis de malware

Si desea excluir cualquier instancia de Amazon EC2 o volumen de Amazon EBS durante el proceso de análisis, puede configurar la etiqueta `GuardDutyExcluded` como `true` para cualquier instancia de Amazon EC2 o volumen de Amazon EBS y GuardDuty no lo analizará. Para obtener más información acerca de las etiquetas de `GuardDutyExcluded`, consulte [Permisos de rol vinculado al servicio para Malware Protection for EC2](#). También puede agregar una etiqueta de instancia de Amazon EC2 a una lista de exclusión. Si agrega varias etiquetas a la lista de exclusión de etiquetas, cualquier instancia de Amazon EC2 que contenga al menos una de estas etiquetas se excluirá del proceso de análisis de malware.

Como cuenta de administrador delegado de GuardDuty, solo puede realizar esta actualización en nombre de las cuentas de miembro de la organización. Sin embargo, si una cuenta de miembro se [administra mediante el método de invitación](#), esta podrá realizar este cambio por su cuenta. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para agregar una etiqueta asociada a una instancia de Amazon EC2 a una lista de exclusión.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, en Planes de protección, elija Protección contra malware para EC2.
3. Amplíe la sección Etiquetas de inclusión/exclusión. Elija Add tags (Añadir etiquetas).
4. Elija Etiquetas de exclusión y, a continuación, elija Confirmar.
5. Especifique el par **Key-Value** de la etiqueta que desee excluir. Es opcional proporcionar el **Value**. Después de agregar todas las etiquetas, elija Guardar.

 Important

Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte [Restricciones de etiquetado](#) en la Guía del usuario de Amazon EC2.

Si no se proporciona un valor para una clave y la instancia de EC2 está etiquetada con la clave especificada, esta instancia de EC2 se excluirá del proceso de análisis de malware iniciado por GuardDuty, independientemente del valor asignado a la etiqueta.

API/CLI

Para ejecutar [UpdateMalwareScanSettings](#), excluya una instancia de EC2 o una carga de trabajo de contenedor del proceso de análisis.

El siguiente comando de ejemplo de la AWS CLI agrega una nueva etiqueta a la lista de exclusión de etiquetas. Sustituya el *detector-id* del ejemplo por su propio detectorId válido.

MapEquals es una lista de pares Key-Value.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
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

Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte [Restricciones de etiquetado](#) en la Guía del usuario de Amazon EC2.

Inclusión de las instancias de EC2 en el análisis de malware

Si desea analizar una instancia de EC2, agregue su etiqueta a la lista de inclusión. Al agregar una etiqueta a una lista de inclusión de etiquetas, las instancias de EC2 que no contengan ninguna de las etiquetas agregadas se omiten del análisis de malware. Si agrega varias etiquetas a la lista de inclusión de etiquetas, se incluirá en el análisis de malware una instancia de EC2 que contenga al menos una de esas etiquetas. A veces, es posible que se omita una instancia de EC2 durante el proceso de análisis por otros motivos. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

Como cuenta de administrador delegado de GuardDuty, solo puede realizar esta actualización en nombre de las cuentas de miembro de la organización. Sin embargo, si una cuenta de miembro se [administra mediante el método de invitación](#), esta podrá realizar este cambio por su cuenta. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para agregar una etiqueta asociada a una instancia de EC2 a una lista de inclusión.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
3. Amplíe la sección Etiquetas de inclusión/exclusión. Elija Add tags (Añadir etiquetas).
4. Elija Etiquetas de inclusión y, a continuación, elija Confirmar.
5. Elija Agregar nueva etiqueta de inclusión y especifique el par de **Key** y **Value** de la etiqueta que desee incluir. Es opcional proporcionar el **Value**.

Una vez que haya agregado todas las etiquetas de inclusión, elija Guardar.

Si no se proporciona un valor para una clave y se etiqueta una instancia de EC2 con la clave especificada, la instancia de EC2 se incluirá en el proceso de análisis de protección contra malware para EC2, independientemente del valor asignado a la etiqueta.

API/CLI

- Ejecute [UpdateMalwareScanSettings](#) para incluir una instancia de EC2 o una carga de trabajo de contenedor en el proceso de análisis.

El siguiente comando de ejemplo de la AWS CLI agrega una nueva etiqueta a la lista de inclusión de etiquetas. Asegúrese de sustituir el *detector-id* de ejemplo por su propio `detectorId` válido. Sustituya la *TestKey* y el *TestValue* de ejemplo por el par Key de y Value de la etiqueta asociada a su recurso de EC2.

`MapEquals` es una lista de pares Key-Value.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
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

Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte [Restricciones de etiquetado](#) en la Guía del usuario de Amazon EC2.

Note

GuardDuty puede tardar hasta cinco minutos en detectar una etiqueta nueva.

En cualquier momento, puede elegir entre etiquetas de inclusión o etiquetas de exclusión, pero no ambas. Si quiere cambiar de una etiqueta a otra, selecciónela en el menú desplegable cuando agregue nuevas etiquetas y confirme su selección. Esta acción borra todas las etiquetas actuales.

Etiqueta **GuardDutyExcluded** global

GuardDuty utiliza una clave de etiqueta global, `GuardDutyExcluded`, que puede agregar a los recursos de Amazon EC2 y establecer el valor de la etiqueta en `true`. Este recurso de Amazon EC2 que tiene este par de clave y valor de etiqueta se excluirá del análisis de malware.

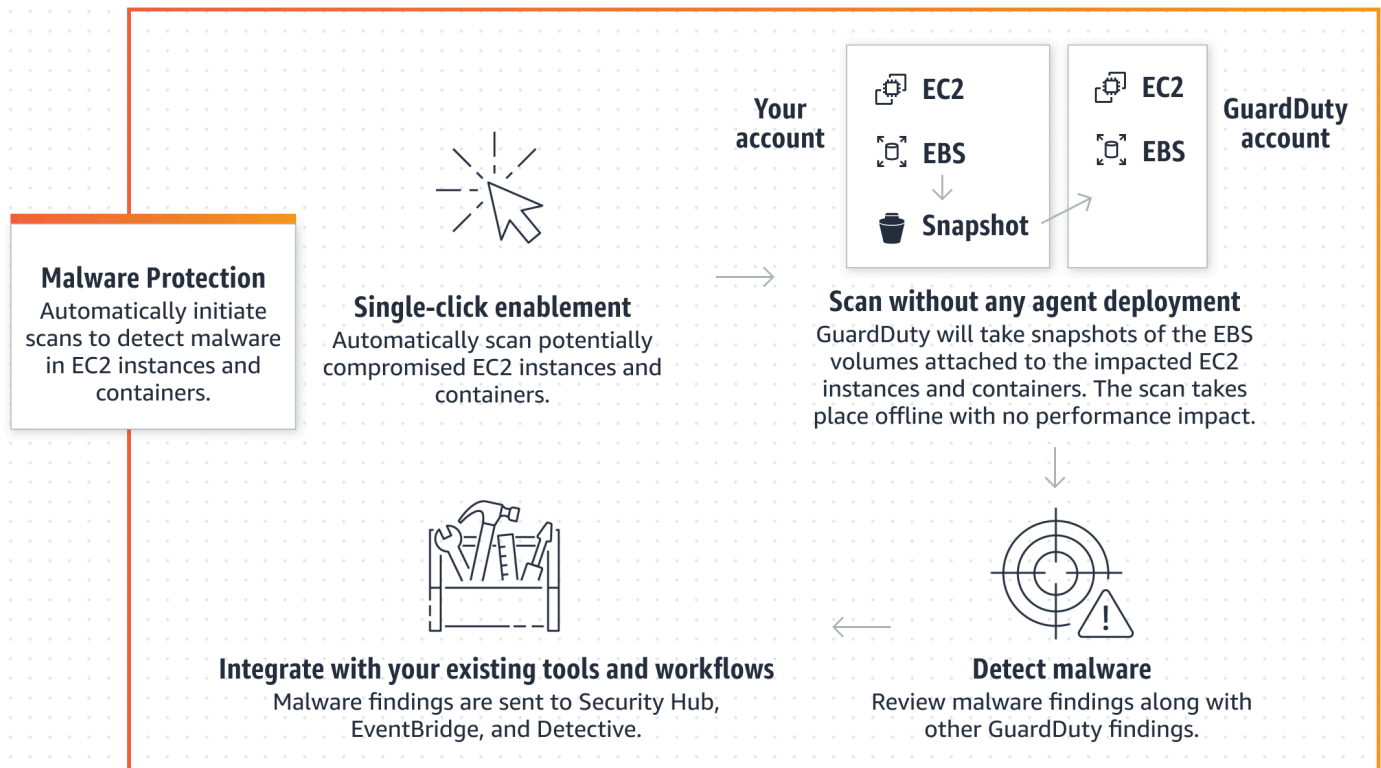
Ambos tipos de análisis (análisis de malware iniciado por GuardDuty y análisis de malware bajo demanda) admiten las etiquetas globales. Si inicia un análisis de malware bajo demanda en Amazon EC2, se generará un ID de análisis. Sin embargo, se omitirá el análisis con un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

Análisis de malware iniciado por GuardDuty

Con el análisis de malware iniciado por GuardDuty habilitado, cada vez que GuardDuty se genera, se inicia [Resultados que invocan un análisis de malware iniciado por GuardDuty](#) un análisis de malware sin agente en los volúmenes de Amazon Elastic Block Store (Amazon EBS) asociados al recurso de Amazon EC2 potencialmente afectado. Antes de que se inicie un análisis, debe preparar la cuenta para cualquier personalización. Las opciones de análisis permiten agregar etiquetas de inclusión para los recursos que desea analizar y etiquetas de exclusión para los recursos que desea omitir durante el proceso de análisis. Al iniciar el análisis automáticamente, siempre se tendrán en cuenta sus opciones de análisis. GuardDuty también admite un par de etiqueta global de clave y valor `GuardDutyExcluded:true`. Al agregar esta etiqueta global a un recurso de Amazon EC2, GuardDuty iniciará el análisis y luego lo omitirá. También puede optar por activar la configuración de retención de instantáneas para retener las instantáneas de los volúmenes de EBS en los que se detectó potencialmente malware. Para obtener más información sobre las opciones de análisis, la etiqueta de exclusión global y la configuración de instantáneas, consulte [Configure la retención de instantáneas y la cobertura de análisis de EC2](#).

Cuando GuardDuty genera múltiples resultados para el mismo recurso de Amazon EC2, GuardDuty podrá iniciar un análisis solo después de que hayan pasado 24 horas desde el último análisis de malware iniciado por GuardDuty. Para obtener información sobre cómo se analizan los volúmenes de Amazon EBS adjuntos a la instancia o carga de trabajo de contenedor de Amazon EC2, consulte [Cómo GuardDuty analiza los volúmenes de EBS para detectar malware](#).

La siguiente imagen describe el funcionamiento del análisis de malware iniciado por GuardDuty.



Para obtener información sobre la metodología de detección de malware de GuardDuty y los motores de análisis que utiliza, consulte [Motor de análisis de detección de malware de GuardDuty](#).

Cuando se encuentra malware, GuardDuty genera [Tipos de resultados de la protección contra malware para EC2](#). Si GuardDuty no genera ningún resultado indicativo de la presencia de malware en el mismo recurso, no se ejecutará ningún análisis de malware iniciado por GuardDuty. También puede iniciar un análisis de malware bajo demanda en el mismo recurso. Para obtener más información, consulte [Análisis de malware bajo demanda en GuardDuty](#).

Prueba gratuita de 30 días en el análisis de malware iniciado por GuardDuty

Puede optar por habilitar o desactivar el análisis de malware iniciado por GuardDuty para una Cuenta de AWS en una Región de AWS compatible en cualquier momento. Si tiene una organización, cada cuenta de miembro tiene su propia prueba gratuita de 30 días.

Para entender cómo funciona la prueba gratuita de 30 días, considere las siguientes situaciones:

- Al habilitar GuardDuty por primera vez (nueva cuenta de GuardDuty), el análisis de malware iniciado por GuardDuty también se habilita y se incluye en la prueba gratuita de 30 días asociada al servicio de GuardDuty.
- Una cuenta de GuardDuty existente puede habilitar el análisis de malware iniciado por GuardDuty por primera vez con una prueba gratuita de 30 días. Cuando se habilita esta característica en una región diferente por primera vez, obtendrá una prueba gratuita de 30 días en esa región.
- Si utilizaba la protección contra malware para EC2 en una Región de AWS antes de que este plan de protección se dividiera en dos tipos de análisis: análisis de malware iniciado por GuardDuty y análisis de malware bajo demanda, aún podrá utilizar el análisis de malware iniciado por GuardDuty con el mismo modelo de precios en la misma Región de AWS. Si habilita el análisis de malware iniciado por GuardDuty por primera vez en una nueva región, la cuenta obtendrá una prueba gratuita de 30 días.

 Note

Aunque se encuentre en un periodo de prueba gratuito de 30 días, se aplica el costo de uso estándar para la creación de las instantáneas de volúmenes de Amazon EBS y su retención. Para obtener más información, consulte [Precios de Amazon EBS](#).

Habilitar el análisis de malware iniciado por GuardDuty en entornos de varias cuentas

En un entorno de varias cuentas, solo la cuenta de administrador de GuardDuty puede habilitar el análisis de malware iniciado por GuardDuty en nombre de sus cuentas de miembro. Además, una cuenta de administrador que administra las cuentas de miembro con compatibilidad con AWS Organizations puede elegir que se habilite automáticamente el análisis de malware iniciado por GuardDuty en todas las cuentas existentes y nuevas en la organización. Para obtener más información, consulte [Administración de cuentas de GuardDuty con AWS Organizations](#).

Establecimiento de un acceso confiable para permitir el análisis de malware iniciado por GuardDuty

Si la cuenta de administrador delegado de GuardDuty no es la misma que la cuenta de administración en la organización, la cuenta de administración debe habilitar el análisis de malware iniciado por GuardDuty para su organización. De esta forma, la cuenta de administrador delegado

puede crear los [Permisos de rol vinculado al servicio para Malware Protection for EC2](#) en las cuentas de miembro que se administran mediante AWS Organizations.

 Note

Antes de designar una cuenta de administrador delegado de GuardDuty, consulte [Recomendaciones y consideraciones](#).

Elija el método de acceso que prefiera para permitir que la cuenta de administrador delegado de GuardDuty habilite el análisis de malware iniciado por GuardDuty para las cuentas de miembro en la organización.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice la cuenta de administración de su organización de AWS Organizations.

2. a. Si no ha designado una cuenta de administrador delegado de GuardDuty, entonces:

En la página Configuración, en cuenta de administrador delegado de GuardDuty, ingrese los 12 dígitos del **account ID** que desee designar para administrar la política de GuardDuty en la organización. Elija Delegar.

- b. i. Si ya designó una cuenta de administrador delegado de GuardDuty diferente de la cuenta de administración, entonces:

En la página Configuración, en Administrador delegado, active la configuración Permisos. Esta acción permitirá a la cuenta de administrador delegado de GuardDuty asociar permisos relevantes a las cuentas de miembro y habilitar el análisis de malware iniciado por GuardDuty en esas cuentas de miembro.

- ii. Si ya ha designado una cuenta de administrador delegado de GuardDuty igual a la cuenta de administración, entonces puede habilitar directamente el análisis de malware iniciado por GuardDuty para las cuentas de miembro. Para obtener más información, consulte [Habilitación automática del análisis de malware iniciado por GuardDuty para todas las cuentas de miembros](#).

 Tip

Si la cuenta de administrador delegado de GuardDuty es diferente de la cuenta de administración, debe otorgar permisos a la cuenta de administrador delegado de GuardDuty para permitir la habilitación del análisis de malware iniciado por GuardDuty para las cuentas de miembro.

3. Si desea permitir que la cuenta de administrador delegado de GuardDuty habilite el análisis de malware iniciado por GuardDuty para cuentas de miembro en otras regiones, cambie la Región de AWS y repita los pasos anteriores.

API/CLI

1. Con sus credenciales de la cuenta de administración, ejecute el siguiente comando:

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (Opcional) para habilitar el análisis de malware iniciado por GuardDuty para la cuenta de administración que no es una cuenta de administrador delegado, la cuenta de administración primero creará los [Permisos de rol vinculado al servicio para Malware Protection for EC2](#) explícitamente en su cuenta y luego habilitará el análisis de malware iniciado por GuardDuty desde la cuenta de administrador delegado, de manera similar a cualquier otra cuenta de miembro.

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. Ha designado la cuenta de administrador delegado de GuardDuty en la Región de AWS actualmente seleccionada. Si ha designado una cuenta como cuenta de administrador delegado de GuardDuty en una región, esa cuenta deberá ser la cuenta de administrador delegado de GuardDuty en todas las demás regiones. Repita el paso anterior para el resto de las regiones.

Configurar el análisis de malware iniciado por GuardDuty para la cuenta de administrador delegado de GuardDuty

Elija el método de acceso que prefiera para habilitar o desactivar el análisis de malware iniciado por GuardDuty para una cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección contra malware para EC2.
3. En la página Protección contra malware para EC2, seleccione Editar junto a Análisis de malware iniciado por GuardDuty.
4. Realice una de las siguientes acciones:

Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las cuentas de GuardDuty activas de su organización de AWS, lo que incluye las nuevas cuentas que se unan a la organización.
- Seleccione Save.

Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de administrador delegado de GuardDuty, elija Configurar cuentas manualmente.
- Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta).
- Seleccione Save.

API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el features del objeto name como EBS_MALWARE_PROTECTION y status como ENABLED.

Para habilitar el análisis de malware iniciado por GuardDuty, puede ejecutar el siguiente comando de la AWS CLI. Asegúrese de utilizar el *ID de detector* válido de la cuenta de administrador delegado de GuardDuty.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /  
    --account-ids 555555555555 /  
    --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Habilitación automática del análisis de malware iniciado por GuardDuty para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la característica de análisis de malware iniciada por GuardDuty en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

Utilizar la página de Protección contra malware para EC2

1. En el panel de navegación, elija Protección contra malware para EC2.
2. En la página Protección contra malware para EC2, elija Editar en la sección Análisis de malware iniciado por GuardDuty.
3. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente el análisis de malware iniciado por GuardDuty para las cuentas existentes y nuevas de la organización.
4. Seleccione Save.

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Análisis de malware iniciado por GuardDuty.
4. En la página Malware Protection for EC2, elija Editar en la sección Análisis de malware iniciado por GuardDuty.
5. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente el análisis de malware iniciado por GuardDuty para las cuentas existentes y nuevas de la organización.
6. Seleccione Save.

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Análisis de malware iniciado por GuardDuty.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitar de forma selectiva del análisis de malware iniciado por GuardDuty para las cuentas de miembro](#).

API/CLI

- Para activar de forma selectiva el análisis de malware iniciado por GuardDuty para las cuentas de miembro, invoque la operación de la API [updateMemberDetectors](#) con el *ID de detector* propio.
- El siguiente ejemplo muestra cómo se puede habilitar el análisis de malware iniciado por GuardDuty para una sola cuenta de miembro. Para deshabilitar una cuenta de miembro, sustituya ENABLED por DISABLED.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación del análisis de malware iniciado por GuardDuty para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar el análisis de malware iniciado por GuardDuty en todas las cuentas de miembros activos existentes en la organización.

Configuración del análisis de malware iniciado por GuardDuty en todas las cuentas de miembros activos existentes

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Malware Protection for EC2.

3. En Malware Protection for EC2, puede ver el estado actual de la configuración del Análisis de malware iniciado por GuardDuty. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Save.

Habilitación automática del análisis de malware iniciado por GuardDuty para todas las cuentas de miembro nuevas

Las cuentas de miembro recién creadas deben Activar GuardDuty antes de seleccionar la configuración del análisis de malware iniciado por GuardDuty. Las cuentas de miembros administradas por invitación pueden configurar manualmente el análisis de malware iniciado por GuardDuty en sus cuentas. Para obtener más información, consulte [Step 3 - Accept an invitation](#).

Elija su método de acceso preferido para habilitar el análisis de malware iniciado por GuardDuty en las cuentas nuevas que se unan a la organización.

Console

La cuenta de administrador delegado de GuardDuty puede habilitar el análisis de malware iniciado por GuardDuty para las nuevas cuentas de miembro en una organización, ya sea a través de la página Malware Protection for EC2 o la página Cuentas.

Habilitación automática del análisis de malware iniciado por GuardDuty para las cuentas de miembro nuevas

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:
 - Utilizar la página Malware Protection for EC2:
 1. En el panel de navegación, elija Malware Protection for EC2.
 2. En la página Malware Protection for EC2, elija Editar en Análisis de malware iniciado por GuardDuty.
 3. Elija Configurar cuentas manualmente.

4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, el análisis de malware iniciado por GuardDuty se habilite automáticamente para la cuenta. Solo la cuenta de administrador delegado de GuardDuty de la organización puede modificar esta configuración.
 5. Seleccione Save.
- Mediante la página Cuentas:
 1. En el panel de navegación, elija Cuentas.
 2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
 3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Análisis de malware iniciado por GuardDuty.
 4. Seleccione Save.

API/CLI

- Para activar o desactivar el análisis de malware iniciado por GuardDuty para las cuentas de miembro nuevas, invoque la operación de la API [UpdateOrganizationConfiguration](#) con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo se puede habilitar el análisis de malware iniciado por GuardDuty para una sola cuenta de miembro. Para deshabilitar esta característica, consulte [Habilitar de forma selectiva del análisis de malware iniciado por GuardDuty para las cuentas de miembro](#). Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `AutoEnable` en `NONE`.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitar de forma selectiva del análisis de malware iniciado por GuardDuty para las cuentas de miembro

Elija su método de acceso preferido para configurar el análisis de malware iniciado por GuardDuty para cuentas de miembros de forma selectiva.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Cuentas.
3. En la página Cuentas, consulte la columna Análisis de malware iniciado por GuardDuty para ver el estado de su cuenta de miembro.
4. Seleccione la cuenta en la que desea configurar el análisis de malware iniciado por GuardDuty. Puede seleccionar varias cuentas de manera simultánea.
5. En el menú Editar planes de protección, elija la opción adecuada para el Análisis de malware iniciado por GuardDuty.

API/CLI

Para activar o desactivar de forma selectiva el análisis de malware iniciado por GuardDuty para las cuentas de miembros, invoque la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.

El siguiente ejemplo muestra cómo se puede habilitar el análisis de malware iniciado por GuardDuty para una sola cuenta de miembro.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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


También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Para habilitar de forma selectiva el análisis de malware iniciado por GuardDuty para las cuentas de miembro, ejecute la operación de la API [updateMemberDetectors](#) con el *ID de detector* propio. El siguiente ejemplo muestra cómo se puede habilitar el análisis de malware iniciado por GuardDuty para una sola cuenta de miembro.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación del análisis de malware iniciado por GuardDuty para las cuentas existentes de la organización administradas mediante invitación

El rol vinculado al servicio (SLR) de Malware Protection for EC2 de GuardDuty se debe crear en las cuentas de miembro. La cuenta de administrador no puede habilitar la característica de análisis de malware iniciada por GuardDuty en las cuentas de miembro que no sean administradas por AWS Organizations.

Actualmente, puede seguir estos pasos a través de la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/> para habilitar el análisis de malware iniciado por GuardDuty en las cuentas de miembros existentes.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta de administrador.

2. En el panel de navegación, elija Cuentas.
3. Seleccione la cuenta de miembro en la que desee habilitar el análisis de malware iniciado por GuardDuty. Puede seleccionar varias cuentas de manera simultánea.
4. Elija Acciones.
5. Seleccione Desasociar miembro.
6. En su cuenta de miembro, seleccione Protección contra malware en Planes de protección, en el panel de navegación.
7. Elija Habilitar análisis de malware iniciado por GuardDuty. GuardDuty creará un SLR para la cuenta de miembro. Para obtener más información sobre los SLR, consulte [Permisos de rol vinculado al servicio para Malware Protection for EC2](#).
8. En la cuenta de administrador, elija Cuentas en el panel de navegación.
9. Elija la cuenta de miembro que debe volver a agregarse a la organización.
10. Seleccione Acciones y Agregar miembro.

API/CLI

1. Utilice la cuenta de administrador para ejecutar la API [DisassociateMembers](#) en las cuentas de miembro que desean habilitar el análisis de malware iniciado por GuardDuty.
2. Utilice su cuenta de miembro para invocar [UpdateDetector](#) y activar el análisis de malware iniciado por GuardDuty.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Utilice la cuenta de administrador para ejecutar la API [CreateMembers](#) y volver a agregar al miembro a la organización.

Habilitar el análisis de malware iniciado por GuardDuty para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar el análisis de malware iniciado por GuardDuty en entornos de varias cuentas](#).

Después de habilitar el análisis de malware iniciado por GuardDuty, GuardDuty iniciará un análisis de malware del volumen de Amazon EBS asociado a la instancia de Amazon EC2 implicada en GuardDuty. Para obtener una lista de los resultados que inician el análisis de malware, consulte [Resultados que invocan un análisis de malware iniciado por GuardDuty](#).

Elija su método de acceso preferido para configurar el análisis de malware iniciado por GuardDuty para una cuenta independiente.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
3. El panel de Malware Protection for EC2 muestra el estado actual del análisis de malware iniciado por GuardDuty para la cuenta. Elija Habilitar para habilitar el análisis de malware iniciado por GuardDuty en esta cuenta.
4. Elija Guardar para confirmar la opción seleccionada.

API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID de detector regional propio y transmita el objeto `dataSources` con `EbsVolumes` establecido en `true`.

También puede habilitar el análisis de malware iniciado por GuardDuty mediante la AWS CLI a través de la ejecución del siguiente comando de la AWS CLI. No olvide utilizar su propio *ID de detector* válido.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Resultados que invocan un análisis de malware iniciado por GuardDuty

Cuando GuardDuty detecta un comportamiento sospechoso que es indicio de la existencia de malware en una instancia de Amazon EC2 o en una carga de trabajo de contenedor que se ejecuta en una instancia de Amazon EC2, GuardDuty generará un resultado. Si este resultado generado pertenece a la siguiente lista de resultados de GuardDuty, GuardDuty iniciará automáticamente un análisis de malware en los volúmenes de Amazon EBS asociados a la instancia de Amazon EC2 implicada en el resultado. Después del análisis, si GuardDuty detecta malware, también generará uno o más [Tipos de resultados de la protección contra malware para EC2](#).

Si se genera alguno de los siguientes resultados de GuardDuty en la cuenta, GuardDuty iniciará automáticamente un análisis de malware en el volumen de Amazon EBS de la instancia de Amazon EC2 potencialmente comprometida.

- [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 salientes)
- [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 salientes)
- [UnauthorizedAccess:EC2/SSHBruteForce](#) (solo salientes)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)

- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)

Análisis de malware bajo demanda en GuardDuty

El análisis de malware bajo demanda le ayuda a detectar la presencia de malware en los volúmenes de Amazon Elastic Block Store (Amazon EBS) asociados a sus instancias de Amazon EC2. Sin necesidad de configuración, puede proporcionar el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2 que desee analizar para iniciar un análisis de malware bajo demanda. Puede iniciar un análisis de malware bajo demanda a través de la consola de GuardDuty o de la API. Antes de iniciar un análisis de malware bajo demanda, puede establecer la configuración de [Retención de instantáneas](#) que prefiera. Los siguientes escenarios pueden ayudarle a identificar cuándo utilizar el tipo de análisis de malware bajo demanda con GuardDuty:

- Desea detectar la presencia de malware en sus instancias de Amazon EC2 sin activar el análisis de malware iniciado por GuardDuty.

- Ha activado el análisis de malware iniciado por GuardDuty y se ha iniciado un análisis automáticamente. Después de seguir la corrección recomendada para el tipo de resultado generado de Malware Protection for EC2, si desea iniciar un análisis en el mismo recurso, podrá iniciar un análisis de malware bajo demanda una vez transcurrida 1 hora desde la hora de inicio del análisis anterior.

El análisis de malware bajo demanda no requiere que hayan transcurrido 24 horas desde el momento en que se inició el análisis de malware anterior. Debería haber transcurrido una hora antes de iniciar un análisis de malware bajo demanda en el mismo recurso. Para evitar la duplicación de un análisis de malware en la misma instancia de EC2, consulte [Volver a analizar una instancia de Amazon EC2 previamente analizada](#).

Note

El análisis de malware bajo demanda no está incluido en el periodo de prueba gratuito de 30 días de GuardDuty. El costo de uso se aplica al volumen total de Amazon EBS analizado por cada análisis de malware. Para más información, consulte [Precios de Amazon GuardDuty](#). Para obtener información sobre el costo de crear las instantáneas del volumen de Amazon EBS y su retención, consulte [Precios de Amazon EBS](#).

Funcionamiento del análisis de malware bajo demanda

Mediante el análisis de malware bajo demanda, puede iniciar una solicitud de análisis de malware para la instancia de Amazon EC2 incluso cuando esté en uso. Tras iniciar un análisis de malware bajo demanda, GuardDuty crea instantáneas de los volúmenes de Amazon EBS asociados a la instancia de Amazon EC2 cuyo nombre de recurso de Amazon (ARN) se ha proporcionado para el análisis. A continuación, GuardDuty comparte estas instantáneas con el [Cuentas de servicio de GuardDuty](#). A partir de estas instantáneas, GuardDuty crea una réplica cifrada de los volúmenes de EBS en la cuenta de servicio. Para obtener más información sobre cómo se analizan los volúmenes de Amazon EBS, consulte [Cómo GuardDuty analiza los volúmenes de EBS para detectar malware](#).

Note

GuardDuty crea instantáneas de los datos que ya se han escrito en los volúmenes de Amazon EBS en el momento en que se inicia un análisis de malware bajo demanda.

Si se encuentra malware y ha activado la configuración de conservación de instantáneas, las instantáneas de su volumen de EBS se retendrán automáticamente en su Cuenta de AWS. El análisis de malware bajo demanda genera el [Tipos de resultados de la protección contra malware para EC2](#). Si no se encuentra ningún malware, las instantáneas de sus volúmenes de EBS se eliminarán, independientemente de la configuración de retención de instantáneas.

GuardDuty utiliza una clave de etiqueta global, `GuardDutyExcluded`, que puede agregar a los recursos de Amazon EC2 y establecer el valor de la etiqueta en `true`. Este recurso de Amazon EC2 que tiene este par de clave y valor de etiqueta se excluirá del análisis de malware. Ambos tipos de análisis (análisis de malware iniciado por GuardDuty y análisis de malware bajo demanda) admiten las etiquetas globales. Si inicia un análisis de malware bajo demanda en Amazon EC2, se generará un ID de análisis. Sin embargo, se omitirá el análisis con un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

Iniciar un análisis de malware bajo demanda en GuardDuty

En esta sección se proporciona una lista de requisitos previos antes de iniciar un análisis de malware bajo demanda y los pasos para iniciar el análisis en un recurso por primera vez.

Como cuenta de administrador de GuardDuty, puede iniciar un análisis de malware bajo demanda en nombre de las cuentas de miembro activas que tengan configurados los siguientes requisitos previos en sus cuentas. Las cuentas independientes y las cuentas de miembro activas en GuardDuty también pueden iniciar un análisis de malware bajo demanda para sus propias instancias de Amazon EC2.

Requisitos previos

Antes de iniciar un análisis de malware bajo demanda, la cuenta debe cumplir los siguientes requisitos previos:

- GuardDuty debe estar habilitado en la Regiones de AWS en la que desea iniciar el análisis de malware bajo demanda.
- Asegúrese de que el [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#) esté asociado al usuario de IAM o rol de IAM. Necesitará la clave de acceso y la clave secreta asociadas al usuario de IAM o rol de IAM.
- Como cuenta de administrador delegado de GuardDuty, tiene la opción de iniciar un análisis de malware bajo demanda en nombre de una cuenta de miembro activa.

- Antes de iniciar un análisis de malware bajo demanda, asegúrese de que no se ha iniciado ningún análisis en el mismo recurso en la última hora; de lo contrario, se eliminará el duplicado. Para obtener más información, consulte [Volver a analizar una instancia de Amazon EC2 previamente analizada](#).
- Si es una cuenta de miembro que no tiene el [Permisos de rol vinculado al servicio para Malware Protection for EC2](#), al iniciar un análisis de malware bajo demanda para una instancia de Amazon EC2 que pertenezca a la cuenta, se creará automáticamente el rol vinculado al servicio para Malware Protection for EC2.

Important

Asegúrese de que nadie elimine los [permisos del rol vinculado al servicio para Malware Protection for EC2](#) cuando el análisis de malware aún esté en curso. Este análisis de malware puede ser iniciado por GuardDuty o iniciado bajo demanda. Eliminar el rol vinculado al servicio impedirá que el análisis se complete correctamente y que se obtenga una conclusión definitiva del análisis.

Iniciar análisis de malware bajo demanda

Puede iniciar un análisis de malware bajo demanda en la cuenta a través de la consola de GuardDuty o mediante la AWS CLI. Deberá proporcionar el nombre de recurso de Amazon (ARN) de Amazon EC2 para el que desea iniciar el análisis. Los pasos detallados se proporcionan tanto en la consola como en las instrucciones de la API/AWS CLI en la siguiente sección.

Elija el método de acceso que prefiera para iniciar un análisis de malware bajo demanda.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. Inicie el análisis mediante una de las siguientes opciones:
 - a. Utilizar la página Malware Protection for EC2:
 - i. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
 - ii. En la página Malware Protection for EC2, proporcione el ARN de la instancia de Amazon EC2¹ para la que desea iniciar el análisis.

- b. Mediante la página Análisis de malware:
 - i. En el panel de navegación, elija Análisis de malware.
 - ii. Elija Iniciar análisis bajo demanda y proporcione el ARN de la instancia de Amazon EC2¹ para la que desea iniciar el análisis.
 - iii. Si se ha vuelto a hacer el análisis, seleccione una ID de instancia de Amazon EC2 en la página Análisis de malware.

Amplíe el menú desplegable Iniciar análisis bajo demanda y seleccione Volver a analizar la instancia seleccionada.

3. Después de iniciar correctamente un análisis con cualquiera de los métodos, se genera una ID de análisis. Puede utilizar este ID de análisis para hacer un seguimiento del progreso del análisis. Para obtener más información, consulte [Supervisión de los estados y resultados de los análisis de malware](#).

API/CLI

Invoque [StartMalwareScan](#) para que acepte el resourceArn de la instancia de Amazon EC2¹ para la que desea iniciar un análisis de malware bajo demanda.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

Tras iniciar correctamente un análisis, StartMalwareScan devuelve un scanId. Invoque [DescribeMalwareScans](#) para supervisar el progreso del análisis iniciado.

¹Para obtener información sobre el formato del ARN de su instancia de Amazon EC2, consulte [Nombre de recurso de Amazon \(ARN\)](#). Para las instancias de Amazon EC2, puede utilizar el siguiente formato de ARN de ejemplo sustituyendo los valores de la partición, la región, la ID de Cuenta de AWS y la ID de la instancia de Amazon EC2. Para obtener información sobre la longitud del ID de instancia, consulte [ID de recursos](#).

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Política de control de servicio de AWS Organizations: acceso denegado

Al utilizar las [políticas de control de servicios \(SCP\)](#) en AWS Organizations, la cuenta de administrador delegado de GuardDuty puede restringir los permisos y denegar acciones, como iniciar un análisis de malware bajo demanda en una instancia de Amazon EC2 propiedad de las cuentas.

Como cuenta de miembro de GuardDuty, al iniciar un análisis de malware bajo demanda para las instancias de Amazon EC2, es posible que reciba un error. Puede conectarse con la cuenta de administración para saber por qué se ha configurado una SCP para su cuenta de miembro. Para más información, consulte [Efectos de las SCP en los permisos](#).

Volver a analizar una instancia de Amazon EC2 previamente analizada

Tanto si el análisis es iniciado por GuardDuty como si es bajo demanda, puede iniciar un nuevo análisis de malware bajo demanda en la misma instancia de Amazon EC2 una hora después de la hora de inicio del análisis de malware anterior. Si el nuevo análisis de malware se inicia en el plazo de 1 hora desde el inicio del análisis de malware anterior, la solicitud producirá el siguiente error y no se generará ningún ID de análisis para esta solicitud.

```
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.
```

Los pasos para volver a analizar la instancia son los mismos que para iniciar un análisis de malware bajo demanda por primera vez. Para obtener más información sobre los pasos, consulte [Iniciar análisis de malware bajo demanda](#).

Para hacer un seguimiento del estado de los análisis de malware, consulte [Supervisión de los estados y resultados de los análisis en Malware Protection for EC2](#).

Supervisión de los estados y resultados de los análisis en Malware Protection for EC2

Tras iniciar un análisis de malware en una instancia de Amazon EC2, GuardDuty proporciona los campos de estado y resultado de manera automática. Puede supervisar el estado durante las transiciones y ver si se ha detectado malware. En la siguiente tabla se muestran los valores posibles asociados al análisis de malware.

Valores potenciales

Running, Completed , Skipped, o bien Failed

Clean or Infected

GuardDuty initiated or On demand

*El resultado del análisis solo se rellena cuando el estado del análisis pasa a ser Completed. El resultado del análisis Infected significa que GuardDuty ha detectado la presencia de malware.

Los resultados de cada análisis de malware tienen un periodo de retención de 90 días. Elija el método de acceso que prefiera para realizar un seguimiento del estado de su análisis de malware.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Análisis de malware en EC2.
3. Puede filtrar los análisis de malware según las siguientes Propiedades disponibles en la barra de criterios de filtro.
 - ID de análisis: identificador único asociado al análisis de malware de EC2.
 - ID de cuenta: ID de la Cuenta de AWS en el que se inició el análisis de malware.
 - ARN de instancia de EC2: nombre de recurso de Amazon (ARN) asociado a la instancia de Amazon EC2 asociada al análisis.
 - Estado del análisis: el estado del análisis del volumen de EBS, como en ejecución, omitido y completado
 - Tipo de análisis: indica si se trata de un análisis de malware bajo demanda o de un análisis de malware iniciado por GuardDuty.

API/CLI

- Una vez que el análisis de malware tenga un resultado, [DescribeMalwareScans](#) puede filtrar los análisis de malware en función de EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS y SCAN_START_TIME.

Los criterios de filtro de GUARDDUTY_FINDING_ID están disponibles cuando GuardDuty inicia el SCAN_TYPE.

- Puede cambiar los *filter-criteria* de ejemplo en el siguiente comando. Actualmente, puede filtrar de una CriterionKey a la vez. Las opciones de CriterionKey son EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS y SCAN_START_TIME.

Puede cambiar los *max-results* (hasta 50) y los *sort-criteria*. El AttributeName es obligatorio y debe ser scanStartTime.

En el ejemplo siguiente, los valores en *rojo* son marcadores de posición. Sustitúyalos por los valores adecuados para la cuenta. Por ejemplo, sustituya el ejemplo detector-id *60b8777933648562554d637e0e4bb3b2* por el detector-id propio y válido. Si utiliza la misma CriterionKey que se muestra a continuación, asegúrese de sustituir el EqualsValue de ejemplo por su propio *scan-id* de AWS válida.

```
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 respuesta de este comando muestra un resultado como máximo con detalles sobre el recurso afectado y los resultados de malware (si está Infected).

Cuentas de servicio de GuardDuty por Región de AWS

Cuando se crea una instantánea y se comparte con una cuenta de servicio de GuardDuty, se crea un nuevo evento en los registros de CloudTrail. Este evento especifica las snapshotId e userId correspondientes (cuenta del servicio de GuardDuty para esa Región de AWS). Para obtener más información, consulte [Cómo GuardDuty analiza los volúmenes de EBS para detectar malware](#).

El siguiente ejemplo es un fragmento de un evento de CloudTrail que muestra el cuerpo de la solicitud de `ModifySnapshotAttribute`:

```
"requestParameters": {
  "snapshotId": "snap-1234567890abcdef0",
  "createVolumePermission": {
    "add": {
      "items": [
        {
          "userId": "111122223333"
        }
      ]
    }
  },
  "attributeType": "CREATE_VOLUME_PERMISSION"
}
```

En la siguiente tabla, se muestran las cuentas de servicio de GuardDuty de cada región. La `userId` es la cuenta de servicio de GuardDuty y depende de la región seleccionada.

Región de AWS	Código de región	ID de cuenta de servicio de GuardDuty (<code>userId</code>)
Este de EE. UU. (Norte de Virginia)	us-east-1	652050842985
Este de EE. UU. (Ohio)	us-east-2	178123968615
Oeste de EE. UU. (Norte de California)	us-west-1	669213148797
Oeste de EE. UU. (Oregón)	us-west-2	447226417196
Asia-Pacífico (Mumbai)	ap-south-1	913179291432
Asia-Pacífico (Osaka)	ap-northeast-3	089661699081
Asia-Pacífico (Seúl)	ap-northeast-2	039163547507
Asia-Pacífico (Tokio)	ap-northeast-1	874749492622

Región de AWS	Código de región	ID de cuenta de servicio de GuardDuty (userId)
Asia-Pacífico (Singapur)	ap-southeast-1	247460962669
Asia-Pacífico (Sídney)	ap-southeast-2	124839743349
Canadá (centro)	ca-central-1	175877067165
Oeste de Canadá (Calgary)	ca-west-1	894794104037
Europa (Fráncfort)	eu-central-1	002294850712
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londres)	eu-west-2	310125036783
Europa (París)	eu-west-3	866607715269
Europa (Estocolmo)	eu-north-1	693780578038
China (Pekín)	cn-north-1	448721096076
China (Ningxia)	cn-northwest-1	480864352451
América del Sur (São Paulo)	sa-east-1	546914126324
Asia-Pacífico (Hyderabad) (Activar)	ap-south-2	682251015962
Asia-Pacífico (Melbourne) (Activar)	ap-southeast-4	353488359550
Asia-Pacífico (Malasia) (Activar)	ap-southeast-5	009160069308
Asia-Pacífico (Tailandia) (Activar)	ap-southeast-7	941377115582

Región de AWS	Código de región	ID de cuenta de servicio de GuardDuty (userId)
Europa (España) (Activar)	eu-south-2	936182149045
Europa (Zúrich) (Activar)	eu-central-2	867642063380
Israel (Tel Aviv) (Activar)	il-central-1	619233833001
Europa (Milán) (Activar)	eu-south-1	977238331021
Asia-Pacífico (Hong Kong) (Activar)	ap-east-1	249472122084
Medio Oriente (Baréin) (Activar)	me-south-1	404001805210
África (Ciudad del Cabo) (Activar)	af-south-1	957664736811
Asia-Pacífico (Yakarta) (Activar)	ap-southeast-3	452118225523
Medio Oriente (EAU) (Activar)	me-central-1	828603743433
México (centro) (Activar)	mx-central-1	557690616787
Asia-Pacífico (Taipéi)	ap-east-2	863518437308
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	226283551151
AWS GovCloud (Oeste de EE. UU.)	us-gov-west-1	226300430612

Cuotas en la protección contra malware de EC2

En esta sección se incluyen las cuotas asociadas al uso de Malware Protection for EC2. Para conocer las cuotas asociadas a GuardDuty, consulte [Cuotas de GuardDuty](#).

En la siguiente tabla se indica la disponibilidad predeterminada de diversos recursos cuando se utiliza Malware Protection for EC2.

Ámbito	Predeterminado/a	Comentarios
Extracción y análisis de datos en un documento comprimido o archivado	5	El número máximo de niveles anidados permitidos en un documento archivado.
Número de documentos dentro de un documento archivado	1 000	El número máximo de archivos que se pueden analizar dentro de un archivo. Este recuento es la suma del número de documentos extraídos del archivo y el número de documentos extraídos de todos los archivos anidados.
Número de amenazas	32	El número máximo de amenazas que se puede ver en el panel de resultados. Es posible que Malware Protection for EC2 de GuardDuty haya detectado más nombres de amenazas. Si el número de nombres de amenazas detectados es superior al valor predeterminado, podrá ver los detalles de JSON cuando seleccione ID de resultado debajo del nombre de resultado en el panel de

Ámbito	Predeterminado/a	Comentarios
		detalles de la consola de GuardDuty.
Número de archivos por amenaza detectada	5	El número máximo de archivos identificados por amenaza detectada. Por ejemplo, si GuardDuty detecta 10 archivos asociados a una sola amenaza, la amenaza mostrará un máximo de 5 archivos.
Volúmenes de EBS por análisis por instancia	11	El número máximo de volúmenes de EBS que GuardDuty puede analizar por instancia de EC2. Si hay más de 11 volúmenes de EBS que necesitan ser analizados, Malware Protection for EC2 de GuardDuty ordena el <code>deviceName</code> alfabéticamente, y selecciona los primeros 11 volúmenes de EBS.

Ámbito	Predeterminado/a	Comentarios
Tamaño del volumen de EBS	2048 GB	Al asociarse a una instancia de Amazon EC2 y a una carga de trabajo de contenedor, Malware Protection for EC2 de GuardDuty puede analizar cada volumen de Amazon EBS que tenga un tamaño de hasta 2048 GB. Esta cuota se aplica a cada Región de AWS en la que se encuentre disponible la compatibilidad con Malware Protection for EC2.
Tipos de sistemas de archivos compatibles	Malware Protection for EC2 de GuardDuty puede analizar los siguientes tipos de sistemas de archivos: • Sistema de archivos de nueva tecnología (NTFS) • Sistema de archivos X (XFS) • Sistema de archivos de segunda extensión (ext2) • Sistema de archivos de cuarta extensión (ext4) • Sistema de archivos con tabla de asignación de archivos (FAT) • Sistema de archivos con tabla de asignación de archivos virtuales (VFAT)	N/A.

Ámbito	Predeterminado/a	Comentarios
Etiquetas de opciones de análisis	50	El máximo número de etiquetas de recursos que puede agregar para personalizar la configuración de las opciones de análisis de malware. Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario .
Periodo de conservación de hallazgos	90	El número máximo de días que GuardDuty conserva un resultado. Para obtener la información más reciente, consulte Cuotas de Amazon GuardDuty .
Periodo de retención de análisis de malware	90	La cantidad máxima de días que Malware Protection for EC2 de GuardDuty retiene el historial de un análisis. Para obtener más información acerca de la visualización de análisis de malware recientes, consulte Supervisión de los estados y resultados de los análisis en Malware Protection for EC2 .
Transacciones por segundo (TPS) para análisis de malware bajo demanda	1	El número de solicitudes de análisis de malware bajo demanda que se pueden iniciar por segundo en cada región.

Ámbito	Predeterminado/a	Comentarios
Límite de ampliación para el análisis de malware bajo demanda	1	El número de solicitudes de análisis de malware bajo demanda simultáneas que se pueden iniciar por segundo en cada región.

Protección contra malware para S3 de GuardDuty

La protección contra malware para S3 ayuda a detectar la posible presencia de malware mediante el análisis de los objetos recién cargados en el bucket seleccionado de Amazon Simple Storage Service (Amazon S3). Cuando un objeto de S3 o una nueva versión de un objeto de S3 existente se carga en el bucket seleccionado, GuardDuty inicia automáticamente un análisis de malware.

[Protección contra malware para S3: descripción general y demostración](#)

Dos enfoques para habilitar la protección contra malware para S3

Puede habilitar la protección contra malware para S3 cuando su Cuenta de AWS habilite el servicio de GuardDuty y utilice la protección contra malware como parte de la experiencia integral de GuardDuty, o al optar por emplear la característica de protección contra malware para S3 de manera independiente, sin habilitar el servicio de GuardDuty. Al habilitar la protección contra malware para S3 por sí misma, se hace referencia a esta en la documentación de GuardDuty como el uso de la protección contra malware para S3 como una característica independiente.

Consideraciones para utilizar la protección contra malware para S3 de forma independiente

- Resultados de seguridad de GuardDuty: el ID de detector es un identificador único asociado a la cuenta en una región. Al habilitar GuardDuty en una o más regiones en una cuenta, se crea automáticamente un ID de detector para esta cuenta en cada región donde GuardDuty se habilita. Para obtener más información, consulte Detector en el documento [Conceptos y términos clave de Amazon GuardDuty](#).

Al habilitar la protección contra malware para S3 de forma independiente en una cuenta, dicha cuenta no tendrá un ID de detector asociado. Esto repercute en las características de GuardDuty que pueden estar a su disposición. Por ejemplo, cuando un análisis de malware de S3 detecta la presencia de malware, no se generará ningún resultado de GuardDuty en la Cuenta de AWS porque todos los resultados de GuardDuty están asociados a un ID de detector.

- Comprobar si el objeto analizado es malicioso: de forma predeterminada, GuardDuty publica los resultados del análisis de malware en el bus de eventos predeterminado de Amazon EventBridge y en un espacio de nombres de Amazon CloudWatch. Si habilita el etiquetado al habilitar la protección contra malware para S3 para un bucket, el objeto de S3 analizado recibe

una etiqueta que menciona la conclusión del análisis. Para obtener más información acerca del etiquetado, consulte [Etiquetado opcional de objetos en función del resultado del análisis](#).

Consideraciones generales para habilitar la protección contra malware para S3

Las siguientes consideraciones generales se aplican tanto si utiliza la protección contra malware para S3 de forma independiente o como parte de la experiencia de GuardDuty:

- Puede habilitar la protección contra malware para S3 para un bucket de Amazon S3 que pertenezca a una cuenta propia. Como cuenta de administrador delegado de GuardDuty no puede habilitar esta característica en un bucket de Amazon S3 que pertenezca a una cuenta de miembro.
- Puede habilitar esta característica en los buckets de S3 que pertenecen a la misma región que está actualmente seleccionada en la consola de GuardDuty. GuardDuty no admite la habilitación de esta característica en buckets de S3 entre regiones.
- Como cuenta de administrador delegado de GuardDuty, recibirá una notificación de Amazon EventBridge cada vez que se produzca un cambio en el [Visualización y explicación del estado del bucket protegido](#) de un bucket de S3 que una de las cuentas de miembro de la organización haya configurado para esta característica.

Contenido

- [Precios y costo de uso de la protección contra malware para S3](#)
- [¿Cómo funciona la protección contra malware para S3?](#)
- [Capacidades de la protección contra malware para S3](#)
- [\(Opcional\) Comience a utilizar la protección contra malware para S3 de GuardDuty de forma independiente \(solo consola\)](#)
- [Configurar la protección contra malware para S3 para el bucket](#)
- [Pasos a seguir tras habilitar la protección contra malware para S3](#)
- [Utilizar el control de acceso basado en etiquetas \(TBAC\) con la protección contra malware para S3](#)
- [Visualización y explicación del estado del bucket protegido](#)
- [Solución de problemas sobre el estado del plan de protección contra malware](#)
- [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#)
- [Editar el plan de protección contra malware para un bucket protegido](#)
- [Desactivar la protección contra malware para S3 para un bucket protegido](#)

- [Compatibilidad con las características de Amazon S3](#)
- [Cuotas en la protección contra malware para S3](#)

Precios y costo de uso de la protección contra malware para S3

Los precios de la protección contra malware para S3 varían con respecto a otros planes de protección en GuardDuty. Mientras que la mayoría de los planes de protección de GuardDuty ofrecen una prueba gratuita de 30 días, la protección contra malware para S3 ofrece un plan de nivel gratuito de 12 meses en AWS. Para obtener información sobre los precios de GuardDuty, consulte [Precios en GuardDuty](#).

En la siguiente lista se indican los precios asociados al uso de la protección contra malware para S3.

Plan de nivel gratuito (costo del análisis)

Cada Cuenta de AWS obtiene un nivel gratuito de 12 meses que incluye el uso hasta un límite específico por mes para cada región. Cada Cuenta de AWS recibe un nivel de uso mensual gratuito de hasta 1000 solicitudes y 1 GB de datos analizados. Si el uso supera el límite especificado, comenzará a incurrir en el costo de uso correspondiente al límite superado. Para obtener información completa sobre los precios, consulte los [precios de los planes de protección de GuardDuty](#).

Para obtener información sobre el costo de uso después de habilitar la protección contra malware para S3, consulte [Revisar el costo de uso de la protección contra malware para S3](#).

Costo de uso del etiquetado de objetos de S3

Al habilitar la protección contra malware para S3, es opcional habilitar el etiquetado para los objetos de S3 analizados. Si decide habilitar el etiquetado de objetos de S3, existe un coste de uso asociado. Para obtener más información sobre los costos, consulte la pestaña [Administración e información](#) en la página de precios de Amazon S3.

El costo de uso del etiquetado de objetos de S3 no está incluido en el plan de nivel gratuito.

API de Amazon S3: costo de uso de GET y PUT

Incurrirá en costos de uso cuando GuardDuty ejecute las API de Amazon S3 basado en el rol de IAM. Por ejemplo, después de asumir el rol de IAM, GuardDuty ejecuta la API `PutObject` para agregar el objeto de prueba al bucket seleccionado. Esto ayuda a GuardDuty a evaluar el estado habilitado de la característica.

Para obtener información sobre los precios de las llamadas a la API de S3 en la Región de AWS, consulte [Solicitudes y recuperaciones de datos en la pestaña Almacenamiento y solicitudes](#) de la página de precios de Amazon S3.

Revisar el costo de uso de la protección contra malware para S3

La cuenta incurrirá en costos de uso cuando se utiliza la protección contra malware para S3 más allá del límite especificado en el plan de nivel gratuito, o al finalizar el periodo de 12 meses del plan de nivel gratuito de la cuenta. Para obtener información sobre el plan de nivel gratuito, consulte [Precios y costo de uso de la protección contra malware para S3](#).

La Consola de GuardDuty no permite revisar el costo de uso de la protección contra malware para S3. Para consultar el costo de uso, vaya al Explorador de costos en la Consola <https://console.aws.amazon.com/costmanagement/>. Para obtener información sobre la facturación de Cuenta de AWS, consulte la [Guía del usuario de AWS Billing](#).

Para obtener información sobre el costo de uso estimado de GuardDuty, consulte [Estimar el costo de uso](#).

¿Cómo funciona la protección contra malware para S3?

En esta sección se describen los componentes de la protección contra malware para S3, cómo funciona después de habilitarla para un bucket de S3 y cómo puede revisar el estado y el producto del análisis de malware.

Descripción general

Puede habilitar la protección contra malware para S3 para un bucket de Amazon S3 que pertenezca a una Cuenta de AWS propia. GuardDuty ofrece la flexibilidad de habilitar esta característica para todo el bucket, o limitar el alcance del análisis de malware a [prefijos de objetos](#) específicos donde GuardDuty analiza cada objeto cargado que comienza con uno de los prefijos seleccionados. Puede agregar hasta 5 prefijos. Cuando se habilita la característica para un bucket de S3, ese bucket se denomina bucket protegido.

Permisos de roles de IAM

La protección contra malware para S3 utiliza un rol de IAM que permite a GuardDuty realizar las acciones de análisis de malware en su nombre. Estas acciones incluyen recibir una notificación de

los objetos recién cargados en el bucket seleccionado, analizar dichos objetos y, opcionalmente, agregar etiquetas a los objetos analizados. Este es un requisito previo para configurar el bucket de S3 con esta característica.

Tiene la opción de actualizar un rol de IAM existente o crear un nuevo rol para este propósito. Al habilitar la protección contra malware para S3 para más de un bucket, podrá actualizar el rol de IAM existente de modo que incluya el nombre del otro bucket, según sea necesario. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).

Etiquetado opcional de objetos en función del resultado del análisis

Al habilitar la protección contra malware para S3 para el bucket, es posible seguir un paso opcional para habilitar el etiquetado de los objetos de S3 analizados. El rol de IAM ya incluye el permiso para agregar etiquetas al objeto después del análisis. Sin embargo, GuardDuty agregará etiquetas solamente cuando habilite esta opción al momento de la configuración.

Debe habilitar esta opción antes de que se cargue un objeto. Una vez finalizado el análisis, GuardDuty agregará una etiqueta predefinida al objeto de S3 analizado con el siguiente par de clave y valor:

GuardDutyMalwareScanStatus:*Potential scan result*

Los posibles valores de la etiqueta del producto del análisis son NO_THREATS_FOUND, THREATS_FOUND, UNSUPPORTED, ACCESS_DENIED y FAILED. Para obtener más información acerca de estos valores, consulte [the section called “Estado potencial de análisis de objeto de S3 y estado del producto”](#).

Habilitar el etiquetado es una de las formas de conocer el producto del análisis del objeto de S3. Además, puede utilizar estas etiquetas para agregar una política de recursos de S3 de control de acceso basado en etiquetas (TBAC), de modo que pueda tomar medidas respecto a los objetos potencialmente maliciosos. Para obtener más información, consulte [Agregar TBAC en el recurso del bucket de S3](#).

Recomendamos que habilite el etiquetado en el momento de configurar la protección contra malware para S3 para el bucket. Si habilita el etiquetado después de que un objeto es cargado y potencialmente se inicia el análisis, GuardDuty no podrá agregar etiquetas al objeto analizado. Para obtener información sobre el costo asociado al etiquetado de objetos de S3, consulte [Precios y costo de uso de la protección contra malware para S3](#).

Proceso posterior a la habilitación de la protección contra malware para S3 para un bucket

Tras habilitar la protección contra malware para S3, se creará un recurso del plan de protección contra malware exclusivo para el bucket de S3 seleccionado. Este recurso está asociado a un ID de plan de protección contra malware, que es un identificador único para el recurso protegido. Al utilizar uno de los permisos de IAM, GuardDuty creará y administrará una regla administrada de EventBridge con el nombre de `D0-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`.

Cómo GuardDuty gestiona los datos: barreras de protección de datos

La protección contra malware para S3 escucha las notificaciones de Amazon EventBridge. Cuando un objeto se carga en el bucket seleccionado o en uno de los prefijos, GuardDuty descarga ese objeto del bucket de S3 por medio de un [AWS PrivateLink](#) y luego lo lee, descifra y analiza en un entorno aislado en la misma región. El entorno de análisis se ejecuta en una nube privada virtual (VPC) bloqueada sin acceso a Internet. La VPC se asocia a un grupo de reglas de firewall de DNS que solo permite la comunicación con los dominios de la lista de permitidos que AWS posee. Durante el análisis, GuardDuty almacena temporalmente el objeto de S3 descargado dentro del entorno de análisis que está cifrado con claves de [AWS Key Management Service\(AWS KMS\)](#).

Note

De forma predeterminada, todas las API de Amazon S3 enumeradas en el [tipo de evento de objeto creado](#) en la Guía del usuario de Amazon S3, iniciarán el análisis de protección contra malware para S3.

Estos tipos de eventos incluyen [PutObject](#), [POST Object](#), [CopyObject](#) y [CompleteMultipartUpload](#).

Para obtener información sobre la metodología de detección de malware de GuardDuty y los motores de análisis que utiliza, consulte [Motor de análisis de detección de malware de GuardDuty](#).

Después de que se complete el análisis de malware, GuardDuty procesará los metadatos del análisis con el estado del análisis y luego eliminará la copia descargada del objeto.

GuardDuty siempre limpia el entorno de análisis antes de que comience un nuevo análisis.

GuardDuty utiliza la autorización contingente para el acceso del operador al entorno de análisis, y cada solicitud de acceso es revisada, aprobada y auditada.

Revisar el estado y el producto del análisis de objetos del S3

GuardDuty publica el evento del producto del análisis del objeto S3 en el bus de eventos predeterminado de Amazon EventBridge. GuardDuty también envía las métricas de análisis, como la cantidad de objetos analizados y los bytes analizados, a Amazon CloudWatch. Si habilitó el etiquetado, GuardDuty agregará la etiqueta predefinida `GuardDutyMalwareScanStatus` y un producto del análisis potencial como valor de la etiqueta.

Important

GuardDuty utiliza una entrega de al menos una vez, lo que significa que puede recibir varios resultados de análisis del mismo objeto. Le recomendamos que diseñe sus aplicaciones para gestionar los resultados duplicados. Solo se le facturará una vez por cada objeto analizado.

Para obtener más información, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).

Revisar los resultados generados

La revisión de los resultados depende de si se utiliza o no la protección contra malware para S3 con GuardDuty. Considere los siguientes escenarios:

Utilizar la protección contra malware para S3 cuando el servicio GuardDuty (ID de detector) esté habilitado

Si el análisis de malware detecta un archivo potencialmente malicioso en un objeto S3, GuardDuty generará un resultado asociado. Puede ver los detalles del resultado y seguir los pasos recomendados para remediarlo potencialmente. Según la [Frecuencia de exportación de resultados](#), los resultados generados se exportan a un bucket de S3 y a un bus de eventos EventBridge.

Para obtener información sobre el tipo de resultado que se generará, consulte [Tipo de resultado de la protección contra malware para S3](#).

Utilizar la protección contra malware para S3 como una característica independiente (sin ID de detector)

GuardDuty no podrá generar resultados porque no hay un ID de detector asociado. Para conocer el estado del análisis de malware del objeto de S3, puede ver el producto del análisis que GuardDuty publica automáticamente en el bus de eventos predeterminado. Además, puede

ver las métricas de CloudWatch para evaluar la cantidad de objetos y bytes que GuardDuty intentó analizar. Puede configurar alarmas de CloudWatch para recibir notificaciones sobre el producto del análisis. Si ha habilitado el etiquetado de objetos de S3, también podrá ver el estado del análisis de malware si comprueba en el objeto de S3 la clave de la etiqueta `GuardDutyMalwareScanStatus` y el valor de la etiqueta del producto del análisis.

Para obtener información sobre el estado y el producto del análisis de objetos de S3, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).

Capacidades de la protección contra malware para S3

La siguiente lista ofrece una descripción general de lo que puede esperar o realizar después de habilitar la protección contra malware para S3 en el bucket:

- Elija qué analizar: analice los archivos a medida que se cargan en todos los prefijos o en prefijos específicos (hasta 5) asociados al bucket de S3 seleccionado.
- Análisis automáticos de objetos cargados: una vez habilitada la protección contra malware para S3 en un bucket, GuardDuty iniciará automáticamente un análisis para detectar malware potencial en cualquier objeto recién cargado.
- Habilitar a través de la consola, mediante API/AWS CLI, o CloudFormation: elija el método que prefiera para habilitar la protección contra malware para S3.

Puede habilitar la protección contra malware para S3 por medio de plataformas de infraestructura como código (IaC), como Terraform. Para obtener más información, consulte [Recurso: `aws\_guardduty\_malware\_protection\_plan`](#).

- Formatos de archivo compatibles, cuotas de la protección contra malware para S3 y características de Amazon S3: la protección contra malware para S3 es compatible con todos los formatos de archivo que se pueden cargar en un bucket de S3. Si el archivo cargado está protegido con contraseña y GuardDuty puede detectar la presencia de protección por contraseña para el tipo de archivo cargado, GuardDuty intentará escanear el contenido original con contraseñas comunes. Si la contraseña falla, se omitirá el análisis. GuardDuty no puede detectar la presencia de protección por contraseña en todos los formatos de archivo. Si GuardDuty no puede detectar la presencia de protección por contraseña, seguirá escaneando el contenido cifrado.

Para obtener información sobre las cuotas relacionadas con el tamaño de los objetos, el nivel máximo de profundidad del archivo y otros detalles, consulte [Cuotas en la protección contra malware para S3](#).

Para obtener información sobre si una característica de Amazon S3 es compatible, consulte [Compatibilidad con las características de Amazon S3](#).

- Admite etiquetar objetos de S3 analizados: al habilitar [Etiquetado opcional de objetos en función del resultado del análisis](#), después de cada análisis de malware, GuardDuty agregará una etiqueta que indica el estado del análisis. Puede utilizar esta etiqueta para configurar el control de acceso basado en etiquetas (TBAC) para los objetos de S3. Por ejemplo, puede restringir el acceso a los objetos de S3 indicados como maliciosos y cuyo valor de etiqueta sea `THREATS_FOUND`.
- Notificaciones de Amazon EventBridge: GuardDuty envía eventos a Amazon EventBridge cuando el estado de los recursos del plan de protección contra malware cambia o se completa un análisis de malware del objeto de S3. Estos eventos se envían al bus de eventos predeterminado. Puede utilizar EventBridge y estos eventos para escribir reglas que realicen acciones, como supervisar cuándo se producen estos eventos. Para obtener más información, consulte [Supervisar análisis de objetos de S3 con Amazon EventBridge](#).
- Métricas de CloudWatch: consulte las métricas de CloudWatch para habilitar alarmas sobre determinados estados de análisis de malware. Para obtener más información, consulte [Métricas de estado de análisis de objetos de S3 en CloudWatch](#).

(Opcional) Comience a utilizar la protección contra malware para S3 de GuardDuty de forma independiente (solo consola)

Siga este paso opcional si desea comenzar a utilizar la opción de detección de amenazas de la protección contra malware para S3 independientemente del estado de GuardDuty en la Cuenta de AWS.

Si también desea utilizar otros planes de protección dedicados en GuardDuty, debe comenzar con el servicio Amazon GuardDuty. Para obtener información sobre los planes de protección de GuardDuty, consulte [Características de GuardDuty](#). Si ya ha habilitado GuardDuty en la cuenta, podrá omitir este paso y continuar con [Configurar la protección contra malware para S3 para el bucket](#).

Pasos para comenzar a utilizar la detección de amenazas de la protección contra malware para S3 únicamente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

2. Seleccione Protección contra malware para S3 únicamente de GuardDuty. Esto ayuda a detectar si un archivo recién cargado en el bucket de Amazon Simple Storage Service (Amazon S3) potencialmente contiene 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. Elija Primeros pasos. Ahora puede continuar con los pasos que se indican en [Configurar la protección contra malware para S3 para el bucket](#).

Configurar la protección contra malware para S3 para el bucket

Para que la protección contra malware para S3 analice y (opcionalmente) agregue etiquetas a los objetos de S3, puede utilizar roles de servicio que tengan los permisos necesarios para realizar acciones de análisis de malware en su nombre. Para obtener más información sobre el uso de roles

de servicio para habilitar la protección contra malware para S3, consulte [Acceso a servicios](#). Este rol es diferente del [rol vinculado al servicio de la protección contra malware de GuardDuty](#).

Si prefiere utilizar roles de IAM, puede asociar un rol de IAM que incluya los permisos necesarios para analizar y (opcionalmente) agregar etiquetas a los objetos de S3. GuardDuty asume entonces este rol de IAM para realizar estas acciones en su nombre. Necesitará este nombre de rol de IAM a la hora de habilitar este plan de protección para el bucket de Amazon S3.

Si utiliza roles de IAM, cada vez que desee proteger un bucket de Amazon S3, deberá seguir los dos pasos que se indican en esta sección.

Para habilitar la protección contra malware para S3, necesitará detalles, como el nombre del bucket de S3, los prefijos de objetos si desea centrar la protección en prefijos específicos y el nombre del rol de IAM con los permisos necesarios.

Los pasos son los mismos tanto si comienza a utilizar la protección contra malware para S3 de forma independiente como si la habilita como parte del servicio de GuardDuty.

Temas

1. [Crear o actualizar la política del rol de IAM](#)
2. [Habilitar la protección contra malware para S3 para el bucket](#)
3. [Solución de problemas de errores de permisos de roles de IAM](#)

Habilitar la protección contra malware para S3 para el bucket

En esta sección se indican los pasos detallados que se deben seguir para habilitar la protección contra malware para S3 en un bucket de una cuenta propia. Revise las siguientes consideraciones antes de continuar:

- Al habilitar este plan de protección mediante la consola GuardDuty, se incluye el paso de crear un nuevo rol o usar un rol existente en la sección Acceso al servicio.
- Si habilita este plan de protección mediante la API o la CLI de GuardDuty, debe [Crear o actualizar la política del rol de IAM](#) antes de continuar.
- Independientemente de cómo habilite este plan de protección, debe tener lo el [Permisos para crear un recurso de plan de protección contra malware](#) requerido.

Pensar la limitación de los buckets de Amazon S3

La limitación de S3 podría limitar la velocidad a la que se pueden transferir datos hacia o desde sus buckets de Amazon S3. Esto podría retrasar los análisis de malware de los objetos recién cargados.

Si espera que sus depósitos de S3 reciban grandes volúmenes de solicitudes de GET y PUT, considere implementar medidas para evitar que se limiten. Para obtener información sobre cómo hacerlo, consulte [Evitar la limitación de Amazon S3](#) en la Guía del usuario de Amazon Athena.

Permisos para crear un recurso de plan de protección contra malware

Al habilitar la protección contra malware para S3 para un bucket de Amazon S3, GuardDuty crea un recurso del plan de protección contra malware que actúa como identificador del plan de protección del bucket. Si aún no utiliza el [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#), debe agregar los siguientes permisos para crear este recurso:

- `guardDuty:CreateMalwareProtectionPlan`
- `iam:PassRole`

Puede usar el siguiente ejemplo de política personalizada y sustituir los *valores de los marcadores de posición* por los valores adecuados para su entorno:

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": "*"   
  }  
]  
}
```

Habilitar la protección contra malware para S3 mediante la Consola de GuardDuty

En las siguientes secciones se explica paso a paso lo que experimentará en la Consola de GuardDuty.

Para habilitar la protección contra malware para S3 mediante la Consola de GuardDuty

Ingresa los detalles del bucket de S3

Siga los pasos que se indican a continuación para proporcionar los detalles del bucket de Amazon S3:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. Por medio del selector Región de AWS que aparece en la esquina superior derecha de la página, seleccione la región en la que desea habilitar la protección contra malware para S3.
3. En el panel de navegación, elija Protección contra malware para S3.
4. En la sección Depósitos protegidos, seleccione Activar para activar la protección contra malware para S3 en un depósito de S3 que le Cuenta de AWS pertenezca.
5. En Ingresar detalles del bucket de S3, ingrese el nombre del bucket de Amazon S3. O bien, seleccione Examinar S3 para seleccionar un bucket de S3.

La Región de AWS del bucket de S3 y la Cuenta de AWS en la que habilite la protección contra malware para S3 deben ser la misma. Por ejemplo, si la cuenta pertenece a la región us-east-1, la región del bucket de Amazon S3 también debe ser us-east-1.

6. En Prefijo, puede seleccionar Todos los objetos del bucket de S3 u Objetos que comiencen con un prefijo específico.

- Seleccione Todos los objetos en el bucket de S3 cuando quiera que GuardDuty pueda analizar todos los objetos recién cargados en el bucket seleccionado.
- Seleccione Objetos que comienzan con un prefijo específico cuando desee analizar los objetos recién cargados que pertenezcan a un prefijo específico. Esta opción sirve para focalizar el alcance del análisis de malware únicamente en los prefijos de objetos seleccionados. Para obtener más información sobre el uso de prefijos, consulte [Organizar objetos en la Consola de Amazon S3 mediante carpetas](#) en la Guía del usuario de Amazon S3.

Elija Agregar prefijo e ingrese el prefijo. Puede agregar hasta cinco prefijos.

Habilite el etiquetado para los objetos analizados

Se trata de un paso opcional. Si habilita la opción de etiquetado antes de que un objeto sea cargado en el bucket, una vez completado el análisis, GuardDuty agregará una etiqueta predefinida con la clave GuardDutyMalwareScanStatus y el valor como resultado del análisis. Para utilizar la protección contra malware para S3 de forma óptima, recomendamos habilitar la opción de agregar etiquetas a los objetos de S3 una vez finalizado el análisis. Se aplica el costo estándar de etiquetado de objetos de S3. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).

Por qué debería habilitar el etiquetado?

- Habilitar el etiquetado es una de las formas de conocer el resultado del análisis de malware. Para obtener información sobre el resultado de un análisis de malware de S3, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).
- Configure la política de control de acceso basado en etiquetas (TBAC) en el bucket de S3 que contiene el objeto potencialmente malicioso. Para obtener información sobre las consideraciones y la forma de aplicar el control de acceso basado en etiquetas (TBAC), consulte [Utilizar el control de acceso basado en etiquetas \(TBAC\) con la protección contra malware para S3](#).

Consideraciones para que GuardDuty agregue una etiqueta al objeto de S:

- De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto. Para obtener más información, consulte [Categorizar el almacenamiento mediante etiquetas](#) en la Guía del usuario de Amazon S3.

Si las 10 etiquetas ya están en uso, GuardDuty no podrá agregar la etiqueta predefinida al objeto analizado. Además, GuardDuty publica el producto del análisis en el bus de eventos predeterminado de EventBridge. Para obtener más información, consulte [Supervisar análisis de objetos de S3 con Amazon EventBridge](#).

- Cuando el rol de IAM seleccionado no incluye el permiso para que GuardDuty etiquete el objeto de S3, aún si el etiquetado está habilitado para el bucket protegido, GuardDuty no podrá agregar etiquetas a este objeto de S3 analizado. Para obtener más información sobre el permiso de rol de IAM necesario para el etiquetado, consulte [Crear o actualizar la política del rol de IAM](#).

Además, GuardDuty publica el producto del análisis en el bus de eventos predeterminado de EventBridge. Para obtener más información, consulte [Supervisar análisis de objetos de S3 con Amazon EventBridge](#).

Para seleccionar una opción en Etiquetar objetos analizados

- Cuando desee que GuardDuty agregue etiquetas a los objetos de S3 analizados, seleccione Etiquetar objetos.
- Cuando no desee que GuardDuty agregue etiquetas a los objetos de S3 analizados, seleccione No etiquetar objetos.

Acceso a los servicios

Siga los pasos que se indican a continuación para elegir un rol de servicio existente o crear un nuevo rol de servicio que cuente con los permisos necesarios para realizar acciones de análisis de malware en su nombre. Entre esas acciones se incluye el análisis de objetos de S3 recién cargados y (opcionalmente) la adición de etiquetas a esos objetos. Para obtener información sobre los permisos que tendrá el rol, consulte [Crear o actualizar la política del rol de IAM](#).

En la sección Acceso al servicio, puede realizar una de las siguientes acciones:

1. Crear y utilizar un nuevo rol de servicio: puede utilizar la opción de crear un nuevo rol de servicio que cuente con los permisos necesarios para realizar el análisis de malware.

En Nombre de rol, puede optar por utilizar el nombre previamente completado por GuardDuty o ingresar un nombre de su elección que signifique algo para identificar el rol. Por ejemplo: `GuardDutyS3MalwareScanRole`. El nombre del rol debe tener entre 1 y 64 caracteres. Los caracteres válidos son a-z, A-Z, 0-9, and '+=, @-_'.

2. Utilizar un rol de servicio existente: puede elegir un rol de servicio existente de la lista Nombre del rol de servicio.
 - a. En Plantilla de política puede ver la política que corresponde al bucket de S3. Asegúrese de que ha ingresado o seleccionado un bucket de S3 en la sección de detalles Ingrese el bucket de S3.
 - b. En Nombre de rol de servicio, elija un rol de servicio de la lista de roles de servicio.

Puede realizar cambios en la política en función de sus necesidades Para obtener más información sobre cómo crear o actualizar un rol de IAM, consulte [Crear o actualizar una política de rol de IAM](#).

Si tiene problemas con los permisos de los roles de IAM, consulte [Solución de problemas de errores de permisos de roles de IAM](#).

(Opcional) Etiquetar el ID del plan de protección contra malware

Este es un paso opcional que ayuda a agregar etiquetas al recurso del plan de protección contra malware que se creará para el recurso de bucket de S3.

Cada etiqueta consta de dos partes: una clave de etiqueta y un valor de etiqueta opcional. Para obtener más información sobre el etiquetado y las ventajas que ofrece, consulte [Etiquetar recursos de AWS](#).

Para agregar etiquetas al recurso del plan de protección contra malware

1. Ingrese la Clave y un Valor opcional para la etiqueta. Tanto la clave como el valor de la etiqueta distinguen entre mayúsculas y minúsculas. Para obtener información sobre los nombres de clave y valor de etiqueta, consulte [Límites y requisitos al asignar nombres a las etiquetas](#).
2. Para agregar más etiquetas al recurso del plan de protección contra malware, seleccione Agregar nueva etiqueta y repita el paso anterior. Puede añadir hasta 50 etiquetas a cada recurso.
3. Seleccione Habilitar.

Habilitar la protección contra malware para S3 mediante la API o la CLI

En esta sección se describen los pasos que se deben seguir para habilitar la protección contra malware para S3 mediante programación en el entorno de AWS. Para esto se requiere el nombre de recurso de Amazon (ARN) del rol de IAM que creó en este paso: [Crear o actualizar la política del rol de IAM](#).

Para habilitar la protección contra malware para S3 mediante programación por medio de la API o la CLI

- Por medio de la API

Ejecute [CreateMalwareProtectionPlan](#) para habilitar la protección contra malware para S3 para un bucket que pertenezca a una cuenta propia.

- Por medio de la AWS CLI

Según cómo desee habilitar la protección contra malware para S3, en la siguiente lista encontrará comandos de ejemplo de la AWS CLI para un caso de uso concreto. Al ejecutar estos comandos, sustituya los *ejemplos de marcadores de posición que aparecen en rojo* por los valores que correspondan a la cuenta.

Comandos de ejemplo de la AWS CLI

- Utilice el siguiente comando de la AWS CLI para habilitar la protección contra malware para S3 para un bucket sin etiquetado para objetos de S3 analizados:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::<111122223333:role/role-name" --protected-resource
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Utilice el siguiente comando de la AWS CLI para habilitar la protección contra malware para S3 para un bucket con prefijos de objeto específicos y sin etiquetado para objetos de S3 analizados:

```
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"]}]'
```

- Utilice el siguiente comando de la AWS CLI para habilitar la protección contra malware para S3 para un bucket con el etiquetado de objetos de S3 analizados habilitado:

```
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"}
```

Después de ejecutar estos comandos correctamente, se generará un ID único de plan de protección contra malware. Para realizar acciones, como actualizar o desactivar el plan de protección del bucket, necesitará este ID de plan de protección contra malware.

Si tiene problemas con los permisos de los roles de IAM, consulte [Solución de problemas de errores de permisos de roles de IAM](#).

Crear o actualizar la política del rol de IAM

Para que la protección contra malware para S3 analice y (opcionalmente) agregue etiquetas a los objetos de S3, puede utilizar roles de servicio que tengan los permisos necesarios para realizar acciones de análisis de malware en su nombre. Para obtener más información sobre el uso de roles de servicio para habilitar la protección contra malware para S3, consulte [Acceso a servicios](#). Este rol es diferente del [rol vinculado al servicio de la protección contra malware de GuardDuty](#).

Si prefiere utilizar roles de IAM, puede asociar un rol de IAM que incluya los permisos necesarios para analizar y (opcionalmente) agregar etiquetas a los objetos de S3. Debe crear un rol de IAM o actualizar un rol existente para incluir estos permisos. Dado que estos permisos son necesarios para cada bucket de Amazon S3 para el que habilite la protección contra malware para S3, deberá seguir este paso para cada bucket de Amazon S3 que desee proteger.

En la siguiente lista se explica cómo ciertos permisos ayudan a GuardDuty a realizar el análisis de malware en su nombre:

- Permita que las acciones de Amazon EventBridge creen y administren la regla administrada de EventBridge para que la protección contra malware para S3 pueda escuchar las notificaciones de los objetos de S3.

Para obtener más información, consulte las [reglas administradas de Amazon EventBridge](#) en la Guía del usuario de Amazon EventBridge.

- Permisa que las acciones de Amazon S3 y EventBridge envíen notificaciones a EventBridge para todos los eventos de este bucket.

Para obtener más información, consulte [Habilitar Amazon EventBridge](#) en la Guía del usuario de Amazon S3.

- Permita que las acciones de Amazon S3 accedan al objeto de S3 cargado y agreguen una etiqueta predefinida, GuardDutyMalwareScanStatus, al objeto de S3 analizado. Al utilizar un prefijo de

objeto, agregue una condición `s3:prefix` únicamente en los prefijos de destino. Esto evita que GuardDuty acceda a todos los objetos de S3 en el bucket.

- Permita que las acciones de clave de KMS accedan al objeto antes de analizar y colocar un objeto de prueba en buckets con el cifrado DSSE-KMS y SSE-KMS admitido.

Note

Este paso es necesario cada vez que habilite la protección contra malware para S3 para un bucket en la cuenta. Si ya cuenta con un rol de IAM existente, puede actualizar su política de forma que incluya los detalles de otro recurso de bucket de Amazon S3. El tema [Agregar permisos de política de IAM](#) proporciona un ejemplo de cómo hacerlo.

Utilice las siguientes políticas para crear o actualizar un rol de IAM.

Políticas

- [Agregar permisos de política de IAM](#)
- [Agregar la política de relación de confianza](#)

Agregar permisos de política de IAM

Puede optar por actualizar la política en línea de un rol de IAM existente o crear un nuevo rol de IAM. Para obtener información sobre los pasos, consulte [Crear un rol de IAM](#) o [Modificar una política de permisos de rol](#) en la Guía del usuario de IAM.

Agregue la siguiente plantilla de permisos al rol de IAM que prefiera. Sustituya los siguientes valores de marcador de posición por los valores apropiados asociados a la cuenta:

- Sustituya *amzn-s3-demo-bucket* por el nombre del bucket de Amazon S3.

Para utilizar el mismo rol de IAM para más de un recurso de bucket de S3, actualice una política existente como se muestra en el siguiente ejemplo:

```
...  
...  
"Resource": [  
    "arn:aws:s3:::amzn-s3-demo-bucket/*",
```



```

        "arn:aws:s3:::amzn-s3-demo-bucket2/*"
    ],
    ...
    ...

```

Asegúrese de agregar una coma (,) antes de agregar un nuevo ARN asociado al bucket de S3. Repita este paso siempre que haga referencia a un Resource de bucket de S3 en la plantilla de política.

- Sustituya **111122223333** por el ID de la Cuenta de AWS.
- Sustituya **us-east-1** por la Región de AWS.
- Sustituya **APKAEIBAERJR2EXAMPLE** por el identificador de clave administrada por el cliente. Si el bucket de S3 está cifrado con una clave de AWS KMS, agregaremos los permisos pertinentes si eligió la opción [Crear un nuevo rol](#) al configurar la protección contra malware para el bucket.

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

Plantilla de la política del rol de 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.guardduty.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"
        }
    }
}
]

```

```
}
```

Agregar la política de relación de confianza

Asocie la siguiente política de confianza al rol de IAM. Para obtener más información sobre los pasos, consulte [Modificar una política de confianza del rol](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Solución de problemas de errores de permisos de roles de IAM

Al activar la protección contra malware para S3, GuardDuty comprueba si su rol de servicio de IAM tiene los permisos necesarios para validar la propiedad del bucket de Amazon S3. Si estos permisos faltan o están mal configurados, es posible que reciba el siguiente mensaje:

```
"message": "The request was rejected because provided IAM role does not have the
required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Los siguientes escenarios pueden ayudarlo a solucionar este error:

Faltan permisos de roles de IAM

- El rol de IAM debe tener los permisos necesarios para permitir la protección contra malware para que S3 asuma el rol.

- GuardDuty valida la propiedad del bucket con el permiso "s3:ListBucket". Debe estar presente en el rol de IAM que se utiliza.

Para obtener información acerca de los permisos, consulte [Crear o actualizar la política del rol de IAM](#).

Disponibilidad del rol de IAM

- Al crear un nuevo rol de IAM, espere unos minutos para que los cambios alcancen una coherencia final antes de activar la protección contra malware para S3. Si intenta activar el plan de protección inmediatamente después de crear el rol, la validación podría fallar.
- Para las implementaciones de infraestructura como código (IaC), GuardDuty recomienda declarar una dependencia de recursos para garantizar que el rol de IAM alcance una coherencia final.

Para ver plantillas de ejemplo sobre cómo hacerlo, consulte el [repositorio GuardDuty en GitHub](#).

Habilitación entre regiones

Compruebe que su bucket de Amazon S3 esté en la misma región en la que está activando la protección contra malware para S3 en GuardDuty.

Pasos a seguir tras habilitar la protección contra malware para S3

En esta sección se indican los pasos que puede seguir tras habilitar la protección contra malware para S3 para un bucket. Los siguientes pasos se presentan en un orden que facilita avanzar en las próximas etapas:

A seguir después de habilitar la protección contra malware para S3 para el bucket

1. Agregue la política de recursos de control de acceso basado en etiquetas (TBAC): al habilitar el etiquetado, antes de cargar un objeto en el bucket seleccionado, asegúrese de agregar la política TBAC al recurso del bucket de S3. Para obtener más información, consulte [Agregar TBAC en el recurso del bucket de S3](#).
2. Supervise el estado del plan de protección contra malware: supervise la columna Estado para cada bucket protegido. Para obtener información sobre los posibles estados y su significado, consulte [Visualización y explicación del estado del bucket protegido](#).
3. Cargar un objeto:

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3>.
2. Cargue un archivo en el bucket de S3 o en el prefijo de objeto para el que habilitó esta característica. Para conocer los pasos para cargar un archivo, consulte [Cargar un objeto en el bucket](#) en la Guía del usuario de Amazon S3.
4. Supervise el estado del análisis del objeto de S3 y el producto del análisis: este paso incluye información sobre cómo comprobar el estado del análisis de malware del objeto de S3.

Habilitados tanto GuardDuty como la protección contra malware para S3	Habilitada únicamente la protección contra malware para S3
• Cuando GuardDuty está habilitado, puede generar el Tipo de resultado de la protección contra malware para S3 para indicar la presencia de malware en el objeto de S3 analizado. • Puede comprobar potencialmente el producto del análisis de objetos de S3 por medio de una o más opciones en Supervisión de los análisis de objetos de S3 en la protección contra malware para S3. Estos incluyen el uso de Amazon EventBridge, las métricas de CloudWatch para el plan de protección contra malware y el etiquetado de objetos analizados.	Puede comprobar potencialmente el producto del análisis de objetos de S3 por medio de una o más opciones en Supervisión de los análisis de objetos de S3 en la protección contra malware para S3. Estos incluyen el uso de Amazon EventBridge, las métricas de CloudWatch para el plan de protección contra malware y el etiquetado de objetos analizados.

Utilizar el control de acceso basado en etiquetas (TBAC) con la protección contra malware para S3

Al habilitar la protección contra malware para S3 para el bucket, podrá optar por habilitar el etiquetado. Después de intentar analizar un objeto de S3 recién cargado en el bucket seleccionado, GuardDuty agregará una etiqueta al objeto analizado para indicar el estado del análisis de malware. Habilitar el etiquetado conlleva un costo de uso directo. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).

GuardDuty utiliza una etiqueta predefinida con la clave como `GuardDutyMalwareScanStatus` y el valor como uno de los estados de análisis de malware. Para obtener información sobre estos valores, consulte [the section called “Estado potencial de análisis de objeto de S3 y estado del producto”](#).

Consideraciones para que GuardDuty agregue una etiqueta al objeto de S:

- De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto. Para obtener más información, consulte [Categorizar el almacenamiento mediante etiquetas](#) en la Guía del usuario de Amazon S3.

Si las 10 etiquetas ya están en uso, GuardDuty no podrá agregar la etiqueta predefinida al objeto analizado. Además, GuardDuty publica el producto del análisis en el bus de eventos predeterminado de EventBridge. Para obtener más información, consulte [Supervisar análisis de objetos de S3 con Amazon EventBridge](#).

- Cuando el rol de IAM seleccionado no incluye el permiso para que GuardDuty etiquete el objeto de S3, aún si el etiquetado está habilitado para el bucket protegido, GuardDuty no podrá agregar etiquetas a este objeto de S3 analizado. Para obtener más información sobre el permiso de rol de IAM necesario para el etiquetado, consulte [Crear o actualizar la política del rol de IAM](#).

Además, GuardDuty publica el producto del análisis en el bus de eventos predeterminado de EventBridge. Para obtener más información, consulte [Supervisar análisis de objetos de S3 con Amazon EventBridge](#).

Agregar TBAC en el recurso del bucket de S3

Puede utilizar las políticas de recursos de bucket de S3 para administrar el control de acceso basado en etiquetas (TBAC) para los objetos de S3. Puede proporcionar acceso a usuarios específicos para acceder y leer el objeto de S3. Si la organización fue creada mediante AWS Organizations, deberá asegurarse de que nadie pueda modificar las etiquetas agregadas por GuardDuty. Para obtener más información, consulte [Impedir que las etiquetas sean modificadas salvo por las entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations. El ejemplo utilizado en el tema vinculado menciona `ec2`. Al utilizar este ejemplo, sustituya `ec2` por `s3`.

En la siguiente lista se explica lo que puede hacer mediante TBAC:

- Impida que todos los usuarios, excepto la entidad principal del servicio de protección contra malware para S3, lean los objetos de S3 que aún no estén etiquetados con el siguiente par de clave y valor de etiqueta:

GuardDutyMalwareScanStatus:*Potential key value*

- Permita que únicamente GuardDuty agregue la clave de etiqueta GuardDutyMalwareScanStatus con valor como producto del análisis a un objeto S3 analizado. La siguiente plantilla de política puede autorizar a determinados usuarios con acceso a anular potencialmente el par de clave y valor de la etiqueta.

Ejemplo de política de recursos del bucket de S:

Sustituya los siguientes valores de marcador en la política de ejemplo:

- *IAM-role-name*: proporciona el rol de IAM que utilizó para configurar la protección contra malware para S3 en el bucket.
- *555555555555*: proporciona la Cuenta de AWS asociada al depósito protegido.
- *amzn-s3-demo-bucket*: proporciona el nombre del bucket protegido.

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"
            }
        }
    }
]
}

```

Podrá obtener más información sobre el etiquetado del recurso S3 en [Etiquetado y políticas de control de acceso](#).

Visualización y explicación del estado del bucket protegido

Después de habilitar la protección contra malware para S3 para un bucket, el estado indica si la característica está configurada y funciona según lo esperado. Este estado está asociado a un identificador (ID) único del plan de protección contra malware. GuardDuty crea este ID en el momento de activar la característica.

Utilice el siguiente procedimiento para ver el estado del bucket protegido:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Protección contra malware para S3.

3. En la tabla de buckets protegidos, consulte la columna de estado correspondiente a su bucket de S3.

En la siguiente tabla se indican y describen los valores del estado asociados al recurso del plan de protección contra malware. Si comprende lo que estos estados significan para su bucket protegido, podrá asegurarse mejor de que GuardDuty inicie un análisis automático de malware cuando se cargue un objeto.

Estado	Descripción
Activa	El bucket de S3 se ha configurado correctamente con la protección contra malware para S3. Cuando el estado es Activo, los cambios en el rol de IAM (eliminación o modificación de permisos) no actualizarán el estado a Advertencia o Error. Recomendamos supervisar el estado del análisis de forma continua mediante cualquiera de los métodos descritos en Supervisión de los análisis de objetos de S3.
Advertencia [*]	La protección contra malware para S3 se diseñó de modo que no se vea afectada cuando aparezca una advertencia. Cuando GuardDuty detecte un nuevo objeto S3, iniciará un análisis de malware. Después de iniciar el análisis correctamente, es posible que el valor de la columna Estado tarde unos minutos en cambiar a Activo. Recibirá una notificación de EventBridge una vez que se actualice el valor de la columna Estado.
Error [*]	El bucket no está protegido. No se completará ninguno de los análisis de malware asociados a este bucket S3. Puede haber una o más causas raíz posibles.

^{*} Para obtener información sobre posibles problemas y los pasos correspondientes para resolverlos, consulte [Solución de problemas sobre el estado del plan de protección contra malware](#).

Solución de problemas sobre el estado del plan de protección contra malware

En el caso de cualquier bucket protegido, GuardDuty muestra el Estado basado en la clasificación. Por ejemplo, si un bucket protegido tiene problemas bajo las categorías de Error y Advertencia, GuardDuty mostrará primero el problema asociado con el estado de Error.

En la siguiente lista aparecen los errores y las advertencias para el estado del plan de protección contra malware.

Errores

- [La notificación de EventBridge está desactivada para este bucket de S3](#)
- [Falta la regla administrada por EventBridge para recibir eventos de buckets de S3](#)
- [El bucket de S3 ya no existe](#)

Advertencia

[No se pudo colocar el objeto de prueba](#)

La notificación de EventBridge está desactivada para este bucket de S3

El código de motivo de estado asociado es

EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED.

Detalle del estado

GuardDuty utiliza EventBridge para recibir una notificación cuando un nuevo objeto se carga en este bucket de S3. Este permiso falta en el rol de IAM.

Pasos para solucionar el problema

Opción 1: agregue la siguiente instrucción de permiso al rol de IAM:

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
```

```
    "arn:aws:s3:::amzn-s3-demo-bucket"  
  ]  
}
```

Sustituya *amzn-s3-demo-bucket* por el nombre del bucket de Amazon S3.

Opción 2: habilite la notificación de EventBridge mediante la Consola de Amazon S3

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3>.
2. En la página Buckets, en la pestaña Buckets de uso general, seleccione el nombre del bucket asociado a este error.
3. En esta página del bucket, elija la pestaña Propiedades.
4. En la sección Amazon EventBridge, seleccione Editar.
5. En la página Editar Amazon EventBridge, en Enviar notificación a Amazon EventBridge para todos los eventos de este bucket, seleccione Activado.
6. Seleccione Save changes (Guardar cambios).

El valor de la columna Estado puede tardar unos minutos en cambiar a Activo.

Falta la regla administrada por EventBridge para recibir eventos de buckets de S3

El código de motivo de estado asociado es EVENTBRIDGE_MANAGED_RULE_DISABLED.

Detalle del estado

Faltan los permisos de la regla administrada EventBridge para administrar la configuración de la regla EventBridge.

Pasos para solucionar el problema

Agregue la siguiente instrucción de permiso al rol de IAM:

```
{  
    "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",  
    "Effect": "Allow",  
    "Action": [  
        "events:PutRule",  
        "events>DeleteRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource": [
        "arn:aws:events:*:*:rule/D0-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ],
    "Condition": {
        "StringEquals": {
            "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
        }
    }
}
```

El valor de la columna Estado puede tardar unos minutos en cambiar a Activo.

El bucket de S3 ya no existe

El código de motivo de estado asociado es `PROTECTED_RESOURCE_DELETED`.

Detalle del estado

Se eliminó este bucket de S3 de la cuenta y ya no existe.

Paso para solucionar el problema

Si la eliminación del bucket de S3 no fue deliberada, puede crear un nuevo bucket desde la consola de Amazon S3.

Después de crear el bucket correctamente, habilite la protección contra malware para S3. Para ello, siga los pasos que se indican en la página [Configurar la protección contra malware para S3 para el bucket](#).

No se pudo colocar el objeto de prueba

El código de motivo de estado asociado es `INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

Note

El permiso para agregar un objeto de prueba es opcional. La ausencia de este permiso en el rol de IAM no impide que la protección contra malware para S3 inicie el análisis de

malware en los objetos recién cargados. Después de que se inicie correctamente un análisis, el estado del plan de protección contra malware puede tardar unos minutos en cambiar de Advertencia a Activo.

Si el rol de IAM ya incluye este permiso, entonces esta advertencia indica una política de bucket de Amazon S3 restrictiva que no permite el acceso de IAM para colocar el objeto de prueba en este bucket de S3.

Detalle del estado

Para validar la configuración del bucket seleccionado, GuardDuty coloca un objeto de prueba en el bucket.

Pasos para solucionar el problema

Puede optar por actualizar el rol de IAM para incluir los permisos que faltan. Agregue los siguientes permisos al rol de IAM seleccionado para que GuardDuty pueda colocar el objeto de prueba en el recurso seleccionado:

```
{
  "Sid": "AllowPutValidationObject",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
  ]
}
```

Sustituya *amzn-s3-demo-bucket* por el nombre del bucket de Amazon S3. Para obtener más información sobre los permisos de roles de IAM, consulte [Crear o actualizar la política del rol de IAM](#).

El valor de la columna Estado puede tardar unos minutos en cambiar a Activo.

Supervisión de los análisis de objetos de S3 en la protección contra malware para S3

Al utilizar la protección contra malware para S3 con un ID de detector de GuardDuty, si el objeto de Amazon S3 es potencialmente malicioso, GuardDuty generará [Tipo de resultado de la protección contra malware para S3](#). Los resultados generados se pueden ver a través de la consola y las API de GuardDuty. Para obtener información para comprender este tipo de resultado, consulte [Detalles de los resultados](#).

Cuando se utiliza la protección contra malware para S3 sin habilitar GuardDuty (sin ID de detector), incluso si el objeto de Amazon S3 analizado es potencialmente malicioso, GuardDuty no podrá generar ningún resultado.

Contenido

- [Estado potencial de análisis de objeto de S3 y estado del producto](#)
- [Supervisar análisis de objetos de S3 con Amazon EventBridge](#)
- [Supervisar los análisis de objetos de S3 con etiquetas administradas por GuardDuty](#)
- [Métricas de estado de análisis de objetos de S3 en CloudWatch](#)

Estado potencial de análisis de objeto de S3 y estado del producto

Esta sección explica los valores potenciales del estado de análisis de objetos de S3 y los valores del producto del análisis.

Un estado de análisis de objeto de S3 indica el estado del análisis de malware, como completado, omitido o fallido.

Un estado del producto del análisis de malware de objeto de S3 indica el producto del análisis basado en el valor del estado del análisis. Cada valor del estado del producto del análisis de malware se asigna a un estado de análisis.

La siguiente lista proporciona los valores potenciales del producto del análisis de objetos de S3. Si ha habilitado el etiquetado, puede supervisar el producto del análisis mediante [Utilizar etiquetas de objetos de S3](#). Después del análisis, el valor de la etiqueta tendrá uno de los siguientes valores del producto del análisis.

Valores potenciales del estado del producto del análisis de malware de objetos de S3.

- **NO_THREATS_FOUND**: GuardDuty no detectó ninguna amenaza potencial asociada al objeto analizado.
- **THREATS_FOUND**: GuardDuty detectó una amenaza potencial asociada al objeto analizado.
- **UNSUPPORTED**: hay algunas razones por las que la protección contra malware para S3 omitirá un análisis. Entre los posibles motivos se incluyen los archivos protegidos con contraseña, los archivos con tasas de compresión extremadamente altas, [Protección contra malware para las cuotas de S3](#) y es posible que no haya compatibilidad con determinadas características de Amazon S3. Para obtener más información, consulte [Capacidades de la protección contra malware para S3](#).
- **ACCESS_DENIED**: GuardDuty no puede acceder a este objeto para realizar un análisis. Compruebe los permisos de rol de IAM asociados a este bucket. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).

Si ha habilitado el etiquetado de objetos de S3 posterior al análisis, consulte [Solucionar errores en el etiquetado posterior al análisis de objetos de S3](#).

- **FAILED**: GuardDuty no puede realizar el análisis de malware en este objeto debido a un error interno.

La siguiente lista proporciona los valores potenciales del estado de análisis de objetos de S3 y su asignación al producto del análisis de objetos de S3.

Valores potenciales del estado de análisis de objetos de S3.

- **Completado**: el análisis se completó correctamente e indica si el objeto S3 tiene malware. En este caso, el valor potencial del producto del análisis de objetos de S3 podría ser **THREATS_FOUND** o **NO_THREATS_FOUND**.
- **Omitido**: GuardDuty omite un análisis de malware cuando el análisis de este objeto de S3 no es compatible con la protección contra malware para S3, o cuando GuardDuty no tiene acceso al objeto de S3 cargado en el bucket seleccionado.

En este caso, el valor potencial del producto del análisis de objetos de S3 podría ser **UNSUPPORTED** o **ACCESS_DENIED**.

GuardDuty también omitirá el análisis si se elimina el rol de IAM requerido.

- Fallido: similar al valor del producto del análisis de objetos de S3 FAILED, este estado de análisis significa que GuardDuty no pudo realizar el análisis de malware en el objeto de S3 debido a un error interno.

Supervisar análisis de objetos de S3 con Amazon EventBridge

Amazon EventBridge: es un bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de varios orígenes. EventBridge proporciona un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS y, luego, dirige dichos datos a destinos como Lambda. Esto le permite monitorear los eventos que ocurren en los servicios y crear arquitecturas basadas en eventos. Para más información, consulte la [Guía del usuario de Amazon EventBridge](#).

Como la cuenta propietaria de un bucket de S3 protegido con protección contra malware para S3, GuardDuty publica notificaciones de EventBridge en el bus de eventos predeterminado en las siguientes situaciones:

- Cambios en el estado de los recursos del plan de protección contra malware para cualquiera de los buckets protegidos. Para obtener información sobre los diversos estados, consulte [Visualización y explicación del estado del bucket protegido](#).

Para configurar una regla de Amazon EventBridge (EventBridge) para el estado de los recursos, consulte [Estado del recurso del plan de protección contra malware](#).

- El producto del análisis de objetos de S3 se publica en el bus de eventos predeterminado de EventBridge.

El campo `s3Throttled` indica si hubo o no un retraso en la carga o recuperación de almacenamiento desde Amazon S3. El valor `true` indica que hubo un retraso, y `false` indica que no hubo retraso.

Si `s3Throttled` es `true` para el producto del análisis, Amazon S3 recomienda configurar los prefijos de manera que ayuden a reducir las transacciones por segundo (TPS) para cada prefijo. Para obtener más información, consulte [Patrones de diseño de prácticas recomendadas: optimización del rendimiento de Amazon S3](#) en la Guía del usuario de Amazon S3.

Para configurar una regla de Amazon EventBridge (EventBridge) para los productos del análisis de objetos de S3, consulte [Producto del análisis del objeto S3](#).

- Se produce un evento de error en la etiqueta posterior al análisis debido a las siguientes razones:

- El rol de IAM no tiene los permisos necesarios para etiquetar el objeto.

La plantilla [Agregar permisos de política de IAM](#) incluye el permiso para que GuardDuty etiquete un objeto.

- El recurso del bucket o el objeto especificado en el rol de IAM ya no existe.
- El objeto de S3 asociado ya ha alcanzado el límite máximo de etiquetas. Para obtener más información sobre el límite de etiquetas, consulte [Categorizar el almacenamiento mediante etiquetas](#) en la Guía del usuario de Amazon S3.

Para configurar una regla de Amazon EventBridge (EventBridge) para los eventos de error en la etiqueta posterior al análisis, consulte [Eventos de error de etiqueta posteriores al análisis](#).

Configurar las reglas de EventBridge

Puede configurar reglas de EventBridge en la cuenta para enviar el estado de los recursos, los eventos de error en la etiqueta posterior al análisis o el producto del análisis de objetos de S3 a otro Servicio de AWS. Como cuenta de administrador delegado de GuardDuty, recibirá la notificación del estado de los recursos del plan de protección contra malware cuando haya un cambio en el estado.

Se aplicará la tarifa estándar de EventBridge. Para obtener más información, consulte [Precios de Amazon EventBridge](#).

Todos los valores que aparecen en *rojo* son marcadores de posición para el ejemplo. Estos valores cambiarán según los valores de la cuenta y según se detecte o no malware.

Temas

- [Estado del recurso del plan de protección contra malware](#)
- [Producto del análisis del objeto S3](#)
- [Eventos de error de etiqueta posteriores al análisis](#)

Estado del recurso del plan de protección contra malware

Puede crear un patrón de eventos de EventBridge basado en las siguientes situaciones:

Valores potenciales de **detail-type**

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"

- "GuardDuty Malware Protection Resource Status Error"

Patrón del evento

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guardduty"]
}
```

Ejemplo de esquema de notificaciones para **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"
  }
}
```

Ejemplo de esquema de notificaciones para **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"
        }
      ]
    }
  }
}

```

Ejemplo de esquema de notificaciones para **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"
      }
    ]
  }
}

```

```
    ]
  }
}
```

Según el motivo de `resourceStatus ERROR`, se completará el valor `statusReasons`.

Para obtener información sobre los pasos de solución de problemas para las siguientes advertencias y errores, consulte [Solución de problemas sobre el estado del plan de protección contra malware](#).

Producto del análisis del objeto S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Ejemplo de esquema de notificaciones para **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
    }
  }
}
```

```

    }
  }
}

```

Ejemplo de esquema de notificaciones para **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

El campo `scanResultDetails.Threats` contiene solo una amenaza. De forma predeterminada, el análisis de protección contra malware para S3 indica la primera amenaza detectada. Después de esto, el `scanStatus` se establece en `COMPLETED`.

Esquema de notificaciones de ejemplo para el estado del producto del análisis **UNSUPPORTED** (Omitido):

```
{
  "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
    }
  }
}
```

Esquema de notificaciones de ejemplo para el estado del producto del análisis **ACCESS_DENIED** (Omitido):

```
{
  "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
    }
  }
}
```

Esquema de notificaciones de ejemplo para el estado del producto del análisis **FAILED**:

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "FAILED",
```



```

    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "FAILED",
      "threats": null
    }
  }
}

```

Eventos de error de etiqueta posteriores al análisis

Patrón del evento:

```

{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty"
}

```

Ejemplo de esquema de notificaciones para **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"
    }]
}
}

```

Ejemplo de esquema de notificaciones para **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"
    }]
  }
}

```

Para solucionar estos motivos de error, consulte [Solucionar errores en el etiquetado posterior al análisis de objetos de S3](#).

Supervisar los análisis de objetos de S3 con etiquetas administradas por GuardDuty

Utilice la opción de habilitar el etiquetado para que GuardDuty pueda agregar etiquetas al objeto de Amazon S3 después de completar el análisis de malware.

Consideraciones para habilitar el etiquetado

- Se aplica un costo de uso asociado cuando GuardDuty etiqueta los objetos de S3. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).
- Debe mantener los permisos de etiquetado requeridos para el rol de IAM que prefiera asociado a este bucket; de lo contrario, GuardDuty no podrá agregar etiquetas a los objetos analizados. El rol de IAM ya incluye los permisos para agregar etiquetas a los objetos de S3 analizados. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).
- De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto de S3. Para obtener más información, consulte [Utilizar el control de acceso basado en etiquetas \(TBAC\)](#).

Después de habilitar el etiquetado para un bucket de S3 o prefijos específicos, cualquier objeto nuevo cargado que sea analizado tendrá una etiqueta asociada en el siguiente formato de par de clave y valor:

GuardDutyMalwareScanStatus:*Scan-Result-Status*

Para obtener información sobre los posibles valores de las etiquetas, consulte [Estado potencial de análisis de objeto de S3 y estado del producto](#).

Solucionar problemas de errores de etiquetas posteriores al análisis de objetos de S3 en la protección contra malware para S3

Esta sección solo se aplica si ha [Habilite el etiquetado para los objetos analizados](#) en el bucket protegido.

Cuando GuardDuty intenta agregar una etiqueta al objeto de S3 analizado, la acción de etiquetar puede resultar en un error. Las posibles razones por las que esto puede ocurrir en el bucket son ACCESS_DENIED y MAX_TAG_LIMIT_EXCEEDED. Utilice los siguientes temas para comprender las posibles razones de estos errores en el etiquetado posterior al análisis y para solucionarlos.

ACCESS_DENIED

La siguiente lista proporciona posibles razones que pueden causar este problema:

- El rol de IAM utilizado para este bucket de S3 protegido no cuenta con el permiso AllowPostScanTag. Verificar que el rol de IAM asociado utilice esta política de bucket. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).
- La política del bucket de S3 protegido no permite que GuardDuty agregue etiquetas a este objeto.
- El objeto de S3 analizado ya no existe.

MAX_TAG_LIMIT_EXCEEDED

De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto de S3. Para obtener más información, consulte Consideraciones para que GuardDuty agregue una etiqueta al objeto de S3 en [Habilite el etiquetado para los objetos analizados](#).

Métricas de estado de análisis de objetos de S3 en CloudWatch

Puede supervisar GuardDuty mediante CloudWatch, que recopila datos originales y los procesa en métricas legibles y casi en tiempo real. Estas estadísticas se retienen durante 15 meses, lo que le permite acceder a información histórica y obtener una mejor perspectiva sobre el rendimiento de la protección contra malware para S3. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulte la [Guía del usuario de Amazon CloudWatch](#).

Las métricas de CloudWatch para la protección contra malware para S3 están disponibles a nivel de recurso. Puede consultar estas métricas por cada recurso protegido de manera independiente. Las métricas se informan en el espacio de nombres AWS/GuardDuty/MalwareProtection. Puede configurar alarmas en recursos específicos para supervisar la postura de seguridad.

Métricas del estado del análisis de malware

Métrica	Descripción
CompletedScanCount	Cantidad de análisis de malware de objetos S3 que se completaron en un periodo determinado.
	Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Unidades: recuento

FailedScanCount

Cantidad de análisis de objetos de S3 maliciosos en los que se produjo un error en un intervalo de tiempo determinado.

Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Unidades: recuento

SkippedScanCount

Cantidad de análisis de malware de objetos de S3 que se omitieron en un periodo determinado.

Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Skipped Reason

Valores potenciales

- Unsupported
- MissingPermissions

Unidades: recuento

Métricas de productos de análisis de malware

InfectedScanCount

La cantidad de análisis de malware en objetos de S3 que detectaron objetos potencialmente maliciosos en un periodo determinado.

Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Unidades: recuento

CompletedScanBytes

La cantidad de bytes de objetos de S3 analizados en un período de tiempo determinado.

Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Unidades: recuento

 Note

De forma predeterminada, las estadísticas en las métricas de CloudWatch son AVG.

Las siguientes dimensiones son compatibles con las métricas de protección contra malware para S3.

Dimensión**Descripción**

ID del plan de protección contra malware

El identificador único asociado con el recurso del plan de protección contra malware que GuardDuty crea para el recurso protegido.

Nombre del recurso	El nombre del recurso protegido.
Razón de la omisión	La razón por la que se ha omitido un análisis de malware de objetos de S3.
	Valores potenciales
	• Unsupported • MissingPermissions

Para obtener información sobre cómo acceder y consultar estas métricas, consulte [Usar métricas de Amazon CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.

Para obtener información sobre la configuración de alarmas, consulte [Utilizar alarmas de Amazon CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.

Editar el plan de protección contra malware para un bucket protegido

Es posible que tenga que editar la política de permisos de IAM que prefiera, habilitar o desactivar el etiquetado del objeto de S3 analizado, o agregar o eliminar prefijos de objetos de S3. Por ejemplo, cuando habilitó la protección contra malware para S3 para el bucket, decidió no habilitar el etiquetado del objeto de S3 analizado con el resultado del análisis. Sin embargo, ahora desea que GuardDuty agregue la etiqueta predefinida y el resultado del análisis como el valor de la etiqueta.

Elija el método de acceso que prefiera para actualizar el plan de protección contra malware para el bucket de S3 protegido.

Console

Para editar un plan de protección contra malware

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección contra malware para S3.
3. En Buckets protegidos, seleccione el bucket para el que desea editar la configuración existente.

4. Seleccione Editar.
5. Actualice la configuración y los ajustes existentes para el bucket y confirme los cambios. Para obtener información sobre la descripción y los pasos de cada sección, consulte [Habilitar la protección contra malware para S3 para el bucket](#).

Supervise la columna Estado correspondiente a este bucket protegido. Si aparece como Advertencia o Error, consulte [Solución de problemas sobre el estado del plan de protección contra malware](#).

API/CLI

Para editar el plan de protección contra malware mediante la API o la AWS CLI

- Mediante la API

Ejecute la API [UpdateMalwareProtectionPlan](#) con el ID del plan de protección contra malware asociado a este recurso del plan.

Para recuperar el ID del plan de protección contra malware en una región específica, puede ejecutar la API [ListMalwareProtectionPlans](#) en esa región.

- Por medio de la AWS CLI

En la siguiente lista se ofrecen comandos de ejemplo de la AWS CLI para actualizar el recurso del plan de protección contra malware. Necesitará el ID del plan de protección contra malware asociado al bucket de S3.

Comandos de ejemplo de la AWS CLI

- Utilice el siguiente comando de la AWS CLI para habilitar o desactivar el etiquetado para el recurso del plan de protección contra malware asociado al bucket de S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
```

- Utilice el siguiente comando de la AWS CLI para agregar un prefijo de objeto al recurso del plan de protección contra malware asociado al bucket de S3:


```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
```

Asegúrese de incluir los prefijos de objeto existentes en este comando; de lo contrario, GuardDuty los eliminará al editar el recurso del plan de protección contra malware.

- Utilice el siguiente comando de la AWS CLI para eliminar un prefijo de objeto del recurso del plan de protección contra malware asociado al bucket de S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
```

Si aún no tiene el ID del plan de protección contra malware para este recurso, puede ejecutar el siguiente comando de la AWS CLI y sustituir *us-east-1* por la región para la que desea enumerar los ID del plan de protección contra malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Desactivar la protección contra malware para S3 para un bucket protegido

Al desactivar la protección contra malware para S3 para un bucket protegido, GuardDuty eliminará el ID del plan de protección contra malware asociado a ese bucket. GuardDuty ya no iniciará un análisis de malware cuando se cargue un nuevo objeto en este bucket o en uno de los prefijos de objetos seleccionados.

Si ha habilitado GuardDuty y ahora desea suspenderlo o desactivarlo, consulte [Suspensión o deshabilitación de GuardDuty](#). Dado que el concepto de ID de detector no existe en la protección contra malware para S3, desactivar o suspender GuardDuty no afectará al estado de un bucket protegido en tu cuenta. Puede continuar el uso de la característica de protección contra malware para S3 de forma independiente con el precio estándar asociado. Para obtener más información, consulte [Revisar el costo de uso de la protección contra malware para S3](#). Para dejar de utilizar la protección contra malware para S3, deberá desactivarla para todos los buckets protegidos en la cuenta. Si desea continuar con el uso de GuardDuty y desactivar únicamente la protección contra

malware para S3 para un bucket, los siguientes pasos no afectarán a la configuración del servicio de GuardDuty ni a otros planes de protección que haya activado.

Elija el método de acceso que prefiera para desactivar la protección contra malware para S3 en el bucket de S3 protegido.

Console

Para desactivar la protección contra malware para S3 mediante la consola de GuardDuty

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección contra malware para S3.
3. En Buckets protegidos, seleccione el bucket para el que desea desactivar la protección contra malware para S3.

Solo puede seleccionar un bucket protegido a la vez. Para desactivar la protección contra malware para S3 para más de un bucket, siga estos pasos de nuevo para otro bucket de S3.

4. Elija Desactivar para confirmar la selección.

API/CLI

Para desactivar la protección contra malware para S3 mediante API o AWS CLI

- Mediante la API

Ejecute la API [DeleteMalwareProtectionPlan](#) con el ID del plan de protección contra malware asociado a este recurso del plan.

Para recuperar el ID del plan de protección contra malware, puede ejecutar la API [ListMalwareProtectionPlans](#).

- Por medio de la AWS CLI

También puede ejecutar el siguiente comando de la AWS CLI para desactivar la protección contra malware para S3. Para ello, sustituya **4cc8bf26c4d75EXAMPLE** por el identificador del plan de protección contra malware asociado a este bucket de S3:

```
aws guardduty delete-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE
```

Si aún no tiene el ID del plan de protección contra malware para este bucket de S3, puede ejecutar el siguiente comando de la AWS CLI y sustituir *us-east-1* por la región para la que desea enumerar los ID del plan de protección contra malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Compatibilidad con las características de Amazon S3

En la siguiente tabla se especifica si la protección contra malware para S3 es compatible o no con las características de Amazon S3 enumeradas.

¿Hay compatibilidad disponible?	Descripción
Sí	Los objetos de S3 se pueden recuperar sin restaurar de forma asíncrona.

¿Hay compatibilidad disponible?	Descripción

¿Hay compatibilidad disponible?	Descripción
Condicional	• La compatibilidad con Intelligent Tiering está disponible para objetos de S3 en los niveles Frequent, Infrequent y Archive Instance Access. • Los niveles de inscripción Archive y Deep Archive no son compatibles. • Intelligent Tiering siempre crea un nuevo objeto en el nivel Frequent Access. Por lo tanto, se admite el análisis de objetos durante la creación. • Las futuras funciones de Intelligent Tiering podrían iniciar los objetos en el nivel Archive. Por lo tanto, esto no se admite.
No	GuardDuty solamente admite buckets de uso general para la protección contra malware para S3.

¿Hay compatibilidad disponible?	Descripción
No	Los objetos de S3 se deben restaurar antes de poder acceder a ellos.
No	La protección contra malware para S3 no se admite en Outposts.

¿Hay compatibilidad disponible?	Descripción
Sí	Todos los objetos de S3 cargados se analizan en busca de malware. Si cargó un objeto con la versión de archivo v1 y, de inmediato, cargó otra versión con v2, GuardDuty analizará ambas versiones del archivo, v1 y v2. Sin embargo, es posible que la hora de inicio del análisis no esté en el mismo orden.
Sí	Si el bucket de destino es un recurso protegido, GuardDuty analizará todos los objetos de S3 replicados en los prefijos protegidos y supervisados.
No	No puede definir una regla de replicación basada en la etiqueta del producto del análisis. Amazon S3 no admite la replicación para etiquetas, excepto durante la creación.

¿Hay compatibilidad disponible?	Descripción
Sí	GuardDuty admite análisis de malware para objetos de S3 cifrados con claves administradas y administradas por el cliente. Asegúrese de que el rol de IAM incluya el permiso para utilizar la clave. Para obtener más información, consulte Agregar permisos de política de IAM.

¿Hay compatibilidad disponible?	Descripción
No	La protección contra malware para S3 no admite el análisis de objetos de S3 cifrados con claves a las que no se puede acceder.
No	Si los objetos de Amazon S3 se cifran mediante el Cliente de cifrado de Amazon S3, no quedarán expuestos a terceros, incluida AWS. Para obtener información sobre por qué no se admite esta opción, consulte Proteger los datos mediante el cifrado del cliente.  Note Los objetos cifrados con CSE-KMS se reciben como un blob cifrado donde no se puede determinar el cifrado. Por lo tanto, GuardDuty los procesa a medida que se reciben y escanea el blob cifrado como un archivo normal. GuardDuty no devuelve el estado de análisis UNSUPPORTED de dichos objetos, a menos que alguno de ellos supere Cuotas en la protección contra malware para S3.

¿Hay compatibilidad disponible?	Descripción
Sí	Los objetos bloqueados de S3 se bloquean según WORM (única escritura, múltiples lecturas). La protección contra malware para S3 puede acceder a los objetos y analizarlos.
Sí	La protección contra malware para S3 puede analizar los buckets configurados con Pago por el solicitante. El solicitante pagará las llamadas a S3. Para obtener más información, consulte Uso de buckets de pagos por solicitante para transferencias de almacenamiento y uso en la Guía del usuario de Amazon S3.
Sí	Puede definir políticas de ciclo de vida basadas en la etiqueta del producto del análisis. Por ejemplo, eliminar automáticamente los objetos maliciosos. Para obtener más información sobre la configuración del ciclo de vida, consulte Administración del ciclo de vida del almacenamiento en la Guía del usuario de Amazon S3.

¿Hay compatibilidad disponible?	Descripción
Sí	Puede definir políticas de recursos de bucket basadas en la etiqueta del producto del análisis de objetos de S3. Por ejemplo, impedir el acceso a objetos de S3 que aún no han sido analizados, o a amenazas detectadas por GuardDuty. Para obtener más información, consulte Utilizar el control de acceso basado en etiquetas (TBAC) con la protección contra malware para S3 .

Cuotas en la protección contra malware para S3

En esta sección se proporcionan las cuotas predeterminadas, que también se conocen como límites. Salvo que se especifique lo contrario, cada cuota es específica de una región. Para consultar las cuotas predeterminadas específicas del uso del servicio GuardDuty fundamental, consulte [Cuotas de Amazon GuardDuty](#).

En las siguientes tablas se describen las cuotas múltiples que se aplicarán a la Cuenta de AWS.

Valor de cuota predeterminado de AWS	¿Se puede ajustar?	Descripción
100 GB	No	El tamaño máximo del objeto de S3 que GuardDuty intentará analizar en busca de malware. Aunque esta cuota no se puede ajustar, si necesita escanear objetos más

Valor de cuota predeterminado de AWS	¿Se puede ajustar?	Descripción
		grandes, póngase en contacto con AWS Support para determinar si GuardDuty puede aumentar la cuota para su caso de uso.
100 GB	No	La cantidad máxima de datos que GuardDuty puede extraer y analizar de un fichero de archivo. GuardDuty omitirá la extracción de archivos de almacenamiento de más de 100 GB.

Valor de cuota predeterminado de AWS	¿Se puede ajustar?	Descripción
10 000	No	La cantidad máxima de archivos que GuardDuty puede extraer y analizar en un fuchero de archivo. Si el archivo contiene más de 10 000 archivos, GuardDuty tendrá que omitir el archivo archivado.  Note Los tipos de archivos compuestos están potencialmente sujetos a estos límites. Los tipos de archivo incluyen, entre otros, mensajes de correo electrónico codificados con extensiones multipropósito de correo de Internet (MIME), archivos Python compilados (PYC), archivos de ayuda HTML compilados (CHM), todos los instaladores y documentos en formato OpenDocument (ODF).
5	No	Los niveles máximos de archivos anidados que GuardDuty puede extraer. Si el archivo incluye archivos anidados más allá de este valor, GuardDuty omitirá esos archivos anidados.

Valor de cuota predeterminado de AWS	¿Se puede ajustar?	Descripción
25	No	La cantidad máxima de buckets de S3 para los que puede habilitar la protección contra malware para S3. Este límite de cuota es por cuenta en cada región.

Protección de RDS de GuardDuty

La protección de RDS en Amazon GuardDuty analiza y elabora perfiles de actividad de inicio de sesión de RDS para detectar posibles amenazas a las [bases de datos de Amazon Aurora](#) (Amazon Aurora compatible con MySQL y Aurora compatible con PostgreSQL) y [Amazon RDS para PostgreSQL](#).

La protección RDS ayuda a identificar comportamientos de inicio de sesión potencialmente sospechosos en estas bases de datos compatibles. GuardDuty monitorea y elabora perfiles [Actividad de inicio de sesión de RDS](#) para actividades anómalas. Por ejemplo, un actor externo previamente inadvertido accede sin autorización a la base de datos, o un adversario intenta acceder por fuerza bruta al intentar adivinar la contraseña de la base de datos.

Con el lanzamiento de la [base de datos ilimitada de Amazon Aurora PostgreSQL](#), GuardDuty amplía RDS Protection para permitir ahora también el monitoreo de la actividad de inicio de sesión desde bases de datos ilimitadas. Si las Cuentas de AWS ya tienen habilitada RDS Protection, GuardDuty empezará automáticamente a monitorear los datos de inicio de sesión de sus bases de datos ilimitadas. En el caso de las cuentas que aún no tienen habilitada la protección RDS, puede obtener más información sobre esta característica [30-day free trial](#) y optar por habilitarla. Para habilitar esta característica, consulte [Habilitar RDS Protection en entornos de varias cuentas](#) o [Habilitar RDS Protection para una cuenta independiente](#).

Nota

Las instancias de réplica de lectura de RDS para PostgreSQL requieren que la instancia de base de datos principal esté en una versión de base de datos compatible y que se replique de manera correcta desde la base de datos principal. Para obtener más información sobre las réplicas de lectura de PostgreSQL, consulte [Trabajo con réplicas de lectura de instancias de base de datos](#) en la Guía del usuario de Amazon RDS.

La protección de RDS no requiere infraestructura adicional; está diseñada para no afectar al rendimiento de las instancias de bases de datos. Cuando RDS Protection detecta un intento de inicio de sesión potencialmente sospechoso o anómalo, GuardDuty genera uno o más [Tipos de resultados de la protección de RDS](#) con detalles sobre la base de datos potencialmente comprometida.

30-Prueba gratuita de 30 días

- Al habilitar GuardDuty en una Cuenta de AWS en una nueva región por primera vez, obtendrá una prueba gratuita de 30 días. En este caso, GuardDuty también habilitará RDS Protection, que está incluida en la prueba gratuita. La protección de RDS empezará a supervisar el comportamiento de inicio de sesión de su base de datos.
- Si ya utiliza GuardDuty y decide habilitar RDS Protection en una nueva región por primera vez, la cuenta de esta región recibirá una prueba gratuita de 30 días para RDS Protection.
- Si ya ha activado RDS Protection, con el lanzamiento de la [base de datos ilimitada de Amazon Aurora PostgreSQL](#) empezará automáticamente a supervisar la actividad de inicio de sesión de las bases de datos ilimitadas. Si su período de prueba gratuito de 30 días de protección de RDS ya ha caducado, empezará a incurrir en gastos de uso relacionados con la supervisión de bases de datos ilimitadas.
- Puede optar por desactivar RDS Protection en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, RDS Protection no se desactivará automáticamente. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Estimar el costo de uso de GuardDuty](#).

Cuando la característica de protección de RDS no está habilitada, GuardDuty no detecta comportamientos de inicio de sesión anómalos o sospechosos. Si desactiva RDS Protection, GuardDuty dejará inmediatamente de supervisar la actividad de inicio de sesión en RDS, y no detectará ninguna amenaza potencial para las instancias de base de datos admitidas ni generará tipos de resultados asociados.

Para que las Regiones de AWS dónde se admiten las bases de datos ilimitadas Aurora PostgreSQL, consulte [Requisitos de la base de datos ilimitados Aurora PostgreSQL](#).

Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles

En la siguiente tabla aparecen las versiones de bases de datos de Aurora y Amazon RDS compatibles con RDS Protection.

Motor de base de datos de Amazon Aurora y Amazon RDS	Versiones del motor admitidas
Aurora MySQL	• 2.10.2 o posteriores • 3.02.1 o posteriores
Aurora PostgreSQL	• 10.23 o posteriores • 11.12 o posteriores • 12.7 o posteriores • 13.3 o posteriores • 14.3 o posteriores • 15.2 o posterior • 16.1 o posterior
RDS para PostgreSQL	• 11.17 o posteriores • 12.12 o posteriores • 13.8 o posteriores • 14.5 o posteriores • RDS para PostgreSQL versión 15 • RDS para PostgreSQL versión 16 • RDS para PostgreSQL versión 17
Base de datos ilimitada de Amazon Aurora PostgreSQL	16.4-limitless

Actividad de inicio de sesión de RDS

Al habilitar la característica de protección de RDS, GuardDuty comenzará a supervisar automáticamente la actividad de inicio de sesión de RDS para las bases de datos, directamente desde los servicios de Aurora y Amazon RDS. La actividad de inicio de sesión de RDS captura los intentos de inicio de sesión correctos y fallidos hechos en la [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) en su entorno de AWS. Si hay indicios de un comportamiento de inicio de sesión anómalo, GuardDuty genera un resultado con detalles de la base de datos potencialmente afectada. Al habilitar RDS Protection por primera vez o al contar con

una instancia de base de datos recién creada, habrá un período de aprendizaje para determinar la referencia de lo que constituye un comportamiento normal. Por esta razón, las instancias de base de datos recién habilitadas o creadas recientemente podrían no generar un resultado de inicio de sesión anómalo asociado hasta después de un período de dos semanas.

Cuando RDS Protection detecta una amenaza potencial, como un patrón inusual en una serie de intentos de inicio de sesión exitosos, fallidos o incompletos, GuardDuty genera uno o más [Tipos de resultados de la protección de RDS](#). Según el tipo de resultado, es posible que se incluyan detalles específicos sobre el comportamiento anómalo, como [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

GuardDuty no administra u actividad de [Bases de datos compatibles](#) o de inicio de sesión de RDS, ni pone a su disposición la actividad de inicio de sesión de RDS.

Habilitar RDS Protection en entornos de varias cuentas

En un entorno de varias cuentas, solo la cuenta del administrador delegado de GuardDuty tiene la opción de habilitar o desactivar la característica de protección de RDS para las cuentas de miembro de la organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro mediante AWS Organizations. Esta cuenta de administrador delegado de GuardDuty puede optar por habilitar automáticamente la supervisión de la actividad de inicio de sesión en RDS para todas las cuentas nuevas a medida que se incorporan a la organización. Para obtener más información sobre entornos de varias cuentas, consulte [Múltiples cuentas en GuardDuty](#).

Habilitar RDS Protection para la cuenta de administrador delegado de GuardDuty

Elija el método de acceso que prefiera para configurar la supervisión de la actividad de inicio de sesión en RDS para la cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección de RDS.
3. En la página Protección de RDS, elija Editar.
4. Realice una de las siguientes acciones:

Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las cuentas de GuardDuty activas de su organización de AWS, lo que incluye las nuevas cuentas que se unan a la organización.
- Seleccione Save.

Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de administrador delegado de GuardDuty, elija Configurar cuentas manualmente.
- Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta).
- Seleccione Save.

API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el features del objeto name como RDS_LOGIN_EVENTS y status como ENABLED.

También puede utilizar la AWS CLI para habilitar RDS Protection. Ejecute el siguiente comando y sustituya `12abc34d567e8fa901bc2d34e56789f0` por el ID de detector de la cuenta y `us-east-1` por la región en la que desea habilitar RDS Protection.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Habilitación automática de RDS Protection para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la característica de protección de RDS en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

Mediante la página Protección de RDS

1. En el panel de navegación, elija Protección de RDS.
2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente RDS Protection para las cuentas nuevas y existentes de la organización.
3. Seleccione Save.

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, elija Habilitar para todas las cuentas en Supervisión de la actividad de inicio de sesión de RDS.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitar RDS Protection para las cuentas de miembro de forma selectiva](#).

API/CLI

Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.

También puede utilizar la AWS CLI para habilitar RDS Protection. Ejecute el siguiente comando y sustituya `12abc34d567e8fa901bc2d34e56789f0` por el ID de detector de la cuenta y `us-east-1` por la región en la que desea habilitar RDS Protection.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de RDS Protection para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar RDS Protection en todas las cuentas de miembros activos existentes en la organización. Las cuentas de miembro que ya tienen GuardDuty habilitado, se conocen como miembros activos existentes.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Protección de RDS.
3. En la página Protección de RDS, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Elija Confirmar.

API/CLI

Ejecute la operación de la API [updateMemberDetectors](#) con el *ID de detector* propio.

También puede utilizar la AWS CLI para habilitar RDS Protection. Ejecute el siguiente comando y sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar RDS Protection.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la Protección de RDS para las cuentas de miembros nuevos

Elija su método de acceso preferido para habilitar la actividad de inicio de sesión de RDS para las cuentas nuevas que se unan a la organización.

Console

La cuenta de administrador delegado de GuardDuty puede habilitar las cuentas de miembro nuevas en una organización a través de la consola, desde la página Protección de RDS o la página Cuentas.

Habilitación automática de la Protección de RDS para las cuentas de miembros nuevos

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

- Mediante la página Protección de RDS:
 1. En el panel de navegación, elija Protección de RDS.
 2. En la página Protección de RDS, elija Editar.
 3. Elija Configurar cuentas manualmente.
 4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, RDS Protection se habilite automáticamente para la cuenta. Solo la cuenta de administrador delegado de GuardDuty de la organización puede modificar esta configuración.
 5. Seleccione Save.
- Mediante la página Cuentas:
 1. En el panel de navegación, elija Cuentas.
 2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
 3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Supervisión de la actividad de inicio de sesión de RDS.
 4. Seleccione Save.

API/CLI

Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API [UpdateOrganizationConfiguration](#) con su propio *ID de detector*.

También puede utilizar la AWS CLI para habilitar RDS Protection. Ejecute el siguiente comando y sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar RDS Protection. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `autoEnable` en `NONE`.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitar RDS Protection para las cuentas de miembro de forma selectiva

Elija el método de acceso que prefiera para habilitar de forma selectiva la supervisión de la actividad de inicio de sesión en RDS para las cuentas de miembro.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas, revise la columna Actividad de inicio de sesión de RDS para ver el estado de su cuenta de miembro.

3. Activación o desactivación de forma selectiva de la actividad de inicio de sesión en RDS

Seleccione la cuenta para la que desee configurar RDS Protection. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione Actividad de inicio de sesión de RDS y, a continuación, elija la opción adecuada.

API/CLI

Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.

También puede utilizar la AWS CLI para habilitar RDS Protection. Ejecute el siguiente comando y sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar RDS Protection.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).


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

 Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitar RDS Protection para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar RDS Protection en entornos de varias cuentas](#).

Tras habilitar RDS Protection, GuardDuty empezará a supervisar [Actividad de inicio de sesión de RDS](#) las bases de datos compatibles en la cuenta.

Elija el método de acceso que prefiera para configurar RDS Protection para una cuenta independiente.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección de RDS.
3. La página Protección de RDS muestra el estado actual de su cuenta. Elija Habilitar para habilitar RDS Protection.
4. Elija Confirmar para guardar su selección.

API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el `features` del objeto `name` como `RDS_LOGIN_EVENTS` y `status` como `ENABLED`.

También puede utilizar la AWS CLI para habilitar RDS Protection. Ejecute el siguiente comando y sustituya `12abc34d567e8fa901bc2d34e56789f0` por el ID de detector de la cuenta y `us-east-1` por la región en la que desea habilitar RDS Protection.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Solución de problemas de monitoreo de protección de RDS

La protección de RDS de GuardDuty analiza y crea perfiles de los eventos de inicio de sesión para detectar posibles amenazas de acceso a las [Bases de datos compatibles](#). Para recopilar la telemetría de seguridad de forma eficaz, GuardDuty requiere que su base de datos esté configurada y funcione sin problemas. Si su base de datos está mal configurada o tiene problemas, es posible que el monitoreo de la seguridad se vea afectado.

En la siguiente sección se describen los problemas más comunes y los pasos para solucionarlos.

Almacenamiento de RDS completo

Si la instancia de RDS se queda sin espacio de almacenamiento, es posible que GuardDuty no recopile datos de telemetría de seguridad. Alcanzar la asignación de capacidad de almacenamiento de instancias de base de datos (`storage-full`) es un estado crítico y RDS recomienda solucionar este problema de inmediato. Para obtener más información, consulte [ver estado de las instancias](#) en la Guía del usuario de Amazon RDS.

Para resolver el estado `storage-full`, puede realizar una de las siguientes acciones:

- Habilitar el escalado automático del almacenamiento (recomendado): active el escalado automático del almacenamiento de Amazon RDS para administrar automáticamente la capacidad de almacenamiento y evitar futuras condiciones de `storage-full`. Para obtener más

información, consulte [Administrar la capacidad de manera automática con el escalado automático de almacenamiento de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

- Monitoree el uso del almacenamiento: verifique el uso del almacenamiento mediante uno de los siguientes métodos:
 - Utilice las métricas de CloudWatch para ver los detalles del almacenamiento. Para obtener más información, consulte [Información de la base de datos de CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.
 - Para ver las métricas de almacenamiento, siga los pasos que se indican en [Monitorear las métricas de una instancia de Amazon RDS](#) en la Guía del usuario de Amazon RDS.
- Modifique la capacidad de almacenamiento: para obtener información sobre cómo aumentar la capacidad de almacenamiento de la instancia, consulte [Aumentar la capacidad de almacenamiento de la instancia de base de datos](#) en la Guía del usuario de Amazon RDS.

Versiones no compatibles en la base de datos principal de RDS para PostgreSQL

Las instancias de réplica de lectura de RDS para PostgreSQL requieren que la instancia de base de datos principal esté en una versión de base de datos compatible y que se replique de manera correcta desde la base de datos principal. GuardDuty monitorea sus instancias solo cuando se cumplen estos requisitos.

Para resolver el problema con la versión no compatible, siga una de estas opciones:

- Verifique la compatibilidad de la versión de la base de datos: verifique que la base de datos principal de RDS para PostgreSQL ejecute una de las versiones compatibles. Para obtener más información, consulte [Bases de datos compatibles](#).
- Solucione un posible problema de replicación: revise y resuelva cualquier problema de replicación entre las instancias principales y de réplica. Para obtener más información sobre cómo realizarlo, consulte [Trabajar con réplicas de lectura para RDS para PostgreSQL](#) en la Guía del usuario de Amazon RDS.

Consideraciones adicionales de seguridad

Si su organización tiene requisitos de cumplimiento estrictos, le recomendamos implementar una auditoría de bases de datos además de utilizar RDS Protection. Para obtener más información sobre

sus responsabilidades de seguridad y su modelo de responsabilidad compartida, consulte [Seguridad en Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Protección de Lambda en GuardDuty

La protección de Lambda lo ayuda a identificar posibles amenazas de seguridad cuando se invoca una función de [AWS Lambda](#) en su entorno de AWS. Al habilitar la protección de Lambda, GuardDuty comienza a supervisar los registros de actividad de red de Lambda. Esto incluye [Logs de flujo de VPC](#) de todas las funciones de Lambda para la cuenta (incluidos los registros que no utilizan redes VPC) y los registros que se generan cuando se invoca la función de Lambda. Cuando GuardDuty identifica tráfico de red sospechoso que indica la presencia de una porción de código potencialmente malicioso en la función de Lambda, GuardDuty genera uno o más [Tipos de resultados de la protección de Lambda](#).

Prueba gratuita de 30 días

En la siguiente lista se explica cómo funciona la prueba gratuita de 30 días para la cuenta:

- Al habilitar GuardDuty en una Cuenta de AWS en una nueva región por primera vez, obtendrá una prueba gratuita de 30 días. En este caso, GuardDuty también habilitará la protección de Lambda, que está incluida en la prueba gratuita.
- Si ya utiliza GuardDuty y decide habilitar la protección de Lambda por primera vez, la cuenta de esta región recibirá una prueba gratuita de 30 días para la protección de Lambda.
- Puede optar por desactivar la protección de Lambda en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, la protección de Lambda no se desactivará automáticamente. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Estimar el costo de uso de GuardDuty](#).

Los registros de actividad de red de Lambda están sujetos a cambios, incluida la ampliación a otra actividad de red, como los datos de consulta de DNS generados al invocar las funciones de Lambda. La expansión a otras formas de supervisión de la actividad de red aumentará el volumen de datos que GuardDuty procesará para la protección de Lambda. Esto afectará directamente al costo de uso de la protección de Lambda. Cada vez que GuardDuty comience a supervisar un registro adicional de la actividad de la red, enviará un aviso a las cuentas que hayan activado la protección de Lambda, al menos 30 días antes del lanzamiento.

 Note

La supervisión de la actividad de red de Lambda no incluye los registros de las [funciones de Lambda@Edge](#).

Supervisión de la actividad de red de Lambda

Cuando se habilita la protección de Lambda, GuardDuty supervisa los registros de actividad de la red de Lambda que se genera cuando se invoca una función de Lambda asociada a la cuenta. Esto lo ayuda a detectar posibles amenazas de seguridad de la función de Lambda. En el caso de las funciones de Lambda que están configuradas para usar redes de VPC, no es necesario habilitar los registros de flujos de VPC para las interfaces de red elásticas (ENI) creadas por Lambda para GuardDuty. GuardDuty solo cobra la cantidad de datos de registros de la actividad de la red de Lambda procesados (en GB) para generar un resultado. GuardDuty optimiza los costos mediante la aplicación de filtros inteligentes y el análisis de un subconjunto de registros de la actividad de la red de Lambda que son relevantes para la detección de amenazas.

GuardDuty no administra los registros de la actividad de la red de Lambda (incluidos los registros de flujos de VPC y no VPC) ni los hace accesibles en la cuenta.

Habilitar la protección de Lambda en entornos de varias cuentas

En un entorno con varias cuentas, solo la cuenta de administrador delegado de GuardDuty tiene la opción de habilitar o desactivar la característica de protección de Lambda para las cuentas de miembro de su organización. Las cuentas de miembros de GuardDuty no pueden modificar esta configuración desde sus cuentas. La cuenta de administrador delegado de GuardDuty administra las cuentas de miembro mediante AWS Organizations. La cuenta de administrador delegado de GuardDuty puede optar por habilitar automáticamente la supervisión de la actividad de red de Lambda para todas las cuentas nuevas que se unan a la organización. Para obtener más información sobre los entornos multicuenta, consulte [Managing multiple accounts in Amazon GuardDuty](#).

Habilitar la protección de Lambda para la cuenta de administrador delegado de GuardDuty

Elija el método de acceso que prefiera para habilitar o desactivar la supervisión de actividad de red de Lambda para la cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, en Configuración, elija Protección de Lambda.
3. En la página Protección de Lambda, seleccione Editar.
4. Realice una de las siguientes acciones:

Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las cuentas de GuardDuty activas de su organización de AWS, lo que incluye las nuevas cuentas que se unan a la organización.
- Seleccione Save.

Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de administrador delegado de GuardDuty, elija Configurar cuentas manualmente.
- Elija Habilitar en la sección Cuenta de administrador delegado de GuardDuty (esta cuenta).
- Seleccione Save.

API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID de detector regional propio y transmita el features del objeto name como LAMBDA_NETWORK_LOGS y el status como ENABLED.

También puede utilizar la AWS CLI para habilitar la protección de Lambda. Ejecute el siguiente comando y sustituya `12abc34d567e8fa901bc2d34e56789f0` por el ID de detector de la cuenta y `us-east-1` por la región en la que desea habilitar la protección de Lambda.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Habilitación automática de la Supervisión de la actividad de red de Lambda para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la característica de supervisión de la actividad de red de Lambda en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

Uso de la página Protección de Lambda

1. En el panel de navegación, elija Protección de Lambda.
2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la supervisión de la actividad de red de Lambda para las cuentas nuevas y existentes de la organización.
3. Seleccione Save.

Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Supervisión de la actividad de red de Lambda.

 Note

De forma predeterminada, esta acción activa automáticamente la opción Habilitar automáticamente GuardDuty para las nuevas cuentas de miembros.

4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros](#).

API/CLI

Para habilitar o deshabilitar la supervisión de la actividad de red de Lambda de forma selectiva para las cuentas de miembros, invoque la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.

También puede utilizar la AWS CLI para habilitar la protección de Lambda. Ejecute el siguiente comando y sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar la protección de Lambda.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes

Elija su método de acceso preferido para habilitar la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes de la organización.

Console

Configuración de la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Protección de Lambda.
3. En la página Protección de Lambda, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Elija Confirmar.

API/CLI

Para habilitar o deshabilitar la supervisión de la actividad de red de Lambda de forma selectiva para las cuentas de miembros, invoque la operación de la API [updateMemberDetectors](#) con su propio *ID de detector*.

También puede utilizar la AWS CLI para habilitar la protección de Lambda. Ejecute el siguiente comando y sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar la protección de Lambda.

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la Supervisión de la actividad de red de Lambda para las nuevas cuentas de miembros

Elija su método de acceso preferido para habilitar la supervisión de la actividad de red de Lambda en las nuevas cuentas de miembros que se unen a la organización.

Console

La cuenta de administrador delegado de GuardDuty puede habilitar la supervisión de la actividad de red de Lambda en las nuevas cuentas miembro de una organización a través de la página de Protección de Lambda o Cuentas.

Habilitación automática de la Supervisión de la actividad de red de Lambda para las nuevas cuentas de miembros

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. Realice una de las siguientes acciones:

- Uso de la página Protección de Lambda:

1. En el panel de navegación, elija Protección de Lambda.
2. En la página Protección de Lambda, seleccione Editar.
3. Elija Configurar cuentas manualmente.
4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se una a su organización, la protección de Lambda se habilitará automáticamente para la cuenta. Solo la cuenta de administrador delegado de GuardDuty de la organización puede modificar esta configuración.
5. Seleccione Save.

- Mediante la página Cuentas:

1. En el panel de navegación, elija Cuentas.

2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las nuevas cuentas en Supervisión de la actividad de red de Lambda.
4. Seleccione Save.

API/CLI

A fin de habilitar la supervisión de la actividad de red de Lambda para las nuevas cuentas de miembro, invoque la operación de la API [UpdateOrganizationConfiguration](#) con el *ID de detector* propio.

También puede utilizar la AWS CLI para habilitar la protección de Lambda. En el siguiente ejemplo se muestra cómo se puede habilitar la supervisión de la actividad de red de Lambda para una sola cuenta de miembro. Sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar la protección de Lambda. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `AutoEnable` en `NONE`.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros

Elija el método de acceso que prefiera para habilitar o deshabilitar de forma selectiva la supervisión de la actividad de red de Lambda en las cuentas de miembros.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, en Configuración, seleccione Cuentas.

En la página Cuentas, revise la columna Supervisión de la actividad de red de Lambda. Indica si la supervisión de la actividad de red de Lambda está habilitada o no.

3. Elija la cuenta para la que desee configurar la protección de Lambda. Puede elegir varias cuentas a la vez.
4. En el menú desplegable Editar planes de protección, elija Supervisión de la actividad de red de Lambda y, a continuación, elija una acción adecuada.

API/CLI

Invoque la API [updateMemberDetectors](#) con su propio *ID de detector*.

También puede utilizar la AWS CLI para habilitar la protección de Lambda. Sustituya *12abc34d567e8fa901bc2d34e56789f0* por el ID de detector de la cuenta y *us-east-1* por la región en la que desea habilitar la protección de Lambda.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitar la protección de Lambda para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en su Cuenta de AWS en una Región de AWS específica.

Si la cuenta está asociada a una cuenta de administrador de GuardDuty a través de AWS Organizations, o por el método de invitación, esta sección no se aplica a la cuenta. Para obtener más información, consulte [Habilitar la protección de Lambda en entornos de varias cuentas](#).

Tras habilitar la protección de Lambda, GuardDuty empezará a supervisar [Supervisión de la actividad de red de Lambda](#) en la cuenta.

Elija el método de acceso que prefiera para configurar la protección de Lambda para una cuenta independiente.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, en Configuración, elija Protección de Lambda.
3. En la página Protección de Lambda se muestra el estado actual de su cuenta. Elija Habilitar para habilitar la protección de Lambda en la cuenta.
4. Elija Confirmar para guardar su selección.

API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID de detector regional propio y transmita el features del objeto name como LAMBDA_NETWORK_LOGS y el status como ENABLED.

También puede utilizar la AWS CLI para habilitar la protección de Lambda. Ejecute el siguiente comando y sustituya **12abc34d567e8fa901bc2d34e56789f0** por el ID de detector de la cuenta y **us-east-1** por la región en la que desea habilitar la protección de Lambda.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

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

Proteger las cargas de trabajo de IA con GuardDuty

La [detección de amenazas básica](#) de Amazon GuardDuty y [Lambda Protection](#) ayudan a aumentar la seguridad y a detectar amenazas para las cargas de trabajo de IA creadas en AWS.

La detección de amenazas básica de GuardDuty monitorea los eventos de administración de AWS CloudTrail para detectar actividades sospechosas y maliciosas en cargas de trabajo de IA generativa creadas mediante el uso de servicios de AWS, incluidos [Amazon Bedrock](#) y [Amazon SageMaker AI](#). Por ejemplo, GuardDuty puede identificar actividades como:

- Supresión inusual de las barreras de protección de seguridad de Amazon Bedrock
- Cambio del origen de los datos de entrenamiento del modelo que puede provocar potencialmente un ataque de envenenamiento de datos.
- Invocación sospechosa del modelo de Amazon Bedrock
- Creación inusual de una instancia de bloc de notas o de un trabajo de entrenamiento en SageMaker AI
- Credenciales de Amazon Elastic Compute Cloud exfiltradas que posiblemente se hayan utilizado para llamar a API en Amazon Bedrock, Amazon SageMaker AI o cargas de trabajo de IA autoadministradas en instancias de EC2, clústeres de EKS o tareas de ECS.

La protección de Lambda de GuardDuty puede ayudar a detectar amenazas potenciales relacionadas con los agentes de Amazon Bedrock. Esto puede incluir actividad sospechosa en la red, como la minería de criptomonedas, y la comunicación con servidores de mando y control maliciosos que pueden ser provocados por un ataque a la cadena de suministro o peticiones complejas.

En el siguiente video se puede ver cómo serían los resultados asociados.

En el siguiente video se puede ver cómo serían los resultados asociados. [Utilizar Amazon GuardDuty para supervisar y reforzar las cargas de trabajo de IA creadas en AWS](#)

Múltiples cuentas en Amazon GuardDuty

Cuando el entorno de AWS tiene varias cuentas, puede administrarlas si designa una Cuenta de AWS como cuenta de administrador. A continuación, podrá asociar las múltiples Cuentas de AWS con esta cuenta de administrador como sus cuentas de miembro. Con esta configuración, una cuenta de administrador de GuardDuty designada puede evaluar y supervisar la seguridad general de la organización. La cuenta de administrador también puede realizar tareas de administración de cuentas, tales como revisar todos los resultados generados y configurar planes de protección dentro de GuardDuty.

En GuardDuty, una organización se compone de una cuenta de administrador delegado de GuardDuty y una o más cuentas de miembro asociadas. Existen dos formas de asociar las cuentas: mediante la integración con AWS Organizations, o a través de un método heredado de envío y aceptación de invitaciones de membresía en la consola de GuardDuty. GuardDuty recomienda que se integre con AWS Organizations.

AWS Organizations es un servicio de administración de cuentas global que permite a los administradores de AWS consolidar y administrar múltiples Cuentas de AWS de forma centralizada. Proporciona características de facturación unificada y administración de cuentas que están diseñadas para satisfacer las necesidades de presupuestos, seguridad y conformidad. Se ofrece sin costo adicional y se integra con varios Servicios de AWS, incluidos Macie, AWS Security Hub CSPM y Amazon GuardDuty. Para obtener más información, consulte la [Guía del usuario de AWS Organizations](#).

Contenido

- [Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro](#)
- [Administración de cuentas de GuardDuty con AWS Organizations](#)
- [Administración de cuentas de GuardDuty por invitación](#)
- [Consideraciones sobre GuardDuty para exportar los detalles de las cuentas de miembro en formato CSV](#)

Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro

Cuando se utiliza GuardDuty en un entorno multicuenta, la cuenta de administrador puede administrar algunos aspectos de GuardDuty en nombre de las cuentas de miembro. Una cuenta de administrador puede realizar las siguientes funciones principales:

- Agregue y elimine cuentas de miembro asociadas: el proceso por el cual una cuenta de administrador puede hacer esto varía según cómo administre las cuentas: a través de AWS Organizations o por el método de invitación de GuardDuty.
- GuardDuty recomienda administrar las cuentas de miembro a través de AWS Organizations.
- La cuenta de administrador delegado de GuardDuty habilita GuardDuty en la cuenta de administración: si la cuenta de administración de AWS Organizations desactiva GuardDuty en algún momento, la cuenta de administrador delegado de GuardDuty podrá habilitar GuardDuty en la cuenta de administración. Sin embargo, es necesario que la cuenta de administración no haya eliminado explícitamente el [Permisos de roles vinculados a servicios de GuardDuty](#).
 - Configure el estado de las cuentas de miembro: una cuenta de administrador puede habilitar o desactivar el estado de los planes de protección de GuardDuty, y habilitar, suspender o desactivar el estado de GuardDuty en nombre de las cuentas de miembro asociadas.

La cuenta de administrador delegado de GuardDuty administrada con AWS Organizations puede habilitar automáticamente GuardDuty cuando las Cuentas de AWS se agregan como miembros.

- Personalice cuándo generar resultados: una cuenta de administrador puede personalizar los resultados dentro de la red de GuardDuty mediante la creación y administración de reglas de supresión, listas de IP de confianza y listas de amenazas. En un entorno de varias cuentas, la compatibilidad para configurar estas características está disponible únicamente para una cuenta de administrador delegado de GuardDuty. Una cuenta de miembro no puede actualizar esta configuración.

En la siguiente tabla se describe la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro.

Clave para la tabla

- Auto: una cuenta solo puede realizar la acción enumerada para su propia cuenta.
- Cualquiera: una cuenta puede realizar la acción enumerada para cualquier cuenta asociada.

- Todas: una cuenta puede realizar la acción enumerada y se aplica a todas las cuentas asociadas. Generalmente, la cuenta que realiza esta acción es una cuenta designada como administrador de GuardDuty
- Celdas con guión (-): las celdas de la tabla con guión (-) indican que la cuenta no puede realizar la acción indicada.

Acción	A través de AWS Organizations		Por invitación	
	Cuenta de administrador delegado de GuardDuty	Cuenta de miembro asociada	Cuenta de administrador de GuardDuty	Cuenta de miembro asociada
Enable GuardDuty	Any	–	Self	Self
Enable GuardDuty automatically for the entire organization (ALL, NUEVO, NONE)	All	–	–	–
View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self

View all GuardDuty findings	Any	Self	Any	Self
Archive GuardDuty findings	Any	—	Any	—
Apply suppression rules	All	—	All	—
Create trusted IP list or threat lists	All	—	All	—
Update trusted IP list or threat lists	All	—	All	—
Delete trusted IP list or threat lists	All	—	All	—
Set EventBridge notification frequency	All	—	All	—
Set Amazon S3 location for exporting findings	All	Self	Self	Self

Habilitar uno o varios planes de protección opcionales para toda la organización (ALL, NEW, NONE)	All	—	—	—
Esto no incluye la protección contra malware para S3.				
Habilitar cualquier plan de protección de GuardDuty para cuentas individuales	Any	—	Any	—
Esto no incluye Malware Protection for EC2 y la protección contra malware para S3.				
Malware Protection for EC2	Any	—	Self	—
Malware Protection for EC2: análisis de malware bajo demanda	Any	Self	Self	Self

Protección contra malware para S3	–	Self	–	Self
Disassociate a member account	Any ⁺	–	Any	–
Disassociate from an administrator account	–	–	–	Self
Delete a disassociated member account	Any	–	Any	–
Suspend GuardDuty	Any [*]	–	Any [*]	–
Disable GuardDuty	Any [*]	–	Any [*]	Self

⁺Indica que la cuenta del administrador de GuardDuty delegado puede realizar esta acción únicamente si no ha configurado la preferencia de habilitación automática a ALL los miembros de la organización.

^{*}Indica que una cuenta de administrador delegado de GuardDuty no puede desactivar GuardDuty en una cuenta de miembro directamente. La cuenta de administrador delegado de GuardDuty debe primero desasociar la cuenta de miembro, y luego eliminarlas. Después de esto, cada cuenta de miembro puede desactivar GuardDuty en sus propias cuentas. Para obtener más información sobre cómo realizar estas tareas en la organización, consulte [Administración continua de las cuentas de miembro en GuardDuty](#).

Administración de cuentas de GuardDuty con AWS Organizations

En una organización de AWS, la cuenta de administración puede designar cualquier cuenta de esta organización como cuenta de administrador delegado de GuardDuty. Para esta cuenta de administrador, GuardDuty se habilita automáticamente solo en la Región de AWS actual. De forma predeterminada, la cuenta de administrador puede habilitar y administrar GuardDuty para todas las

cuentas de miembro de la organización dentro de esa región. La cuenta de administrador puede ver y agregar miembros a esta organización de AWS.

En las siguientes secciones se explican varias tareas que puede realizar como cuenta de administrador delegado de GuardDuty.

Contenido

- [Consideraciones y recomendaciones para utilizar GuardDuty con AWS Organizations](#)
- [Permisos necesarios para designar una cuenta de administrador delegado de GuardDuty](#)
- [Designar una cuenta de administrador delegado de GuardDuty](#)
- [Configuración de las preferencias de habilitación automática de la organización](#)
- [Cómo agregar miembros a la organización](#)
- [\(Opcional\) Habilitar planes de protección para cuentas de miembro existentes](#)
- [Administración continua de las cuentas de miembro en GuardDuty](#)
- [Suspender GuardDuty para la cuenta de miembro](#)
- [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#)
- [Eliminar cuentas de miembro de la organización de GuardDuty](#)
- [Cambiar la cuenta de administrador delegado de GuardDuty](#)

Consideraciones y recomendaciones para utilizar GuardDuty con AWS Organizations

Las siguientes consideraciones y recomendaciones resultan útiles para comprender el funcionamiento de una cuenta de administrador delegado en GuardDuty:

Una cuenta de administrador delegado de GuardDuty puede administrar un máximo de 50 000 miembros.

Existe un límite de 50 000 cuentas de miembro por cuenta de administrador delegado de GuardDuty. Esto incluye cuentas de miembro que se agregan a través de AWS Organizations o aquellas que aceptaron la invitación de la cuenta de administrador de GuardDuty para unirse a su organización. Sin embargo, es posible que en la organización de AWS haya más de 50 000 cuentas.

Si excede el límite de 50 000 cuentas de miembro, recibirá una notificación de CloudWatch, AWS Health Dashboard, y un correo electrónico a la cuenta de administrador delegado de GuardDuty designada.

Una cuenta de administrador delegado de GuardDuty es regional.

A diferencia de AWS Organizations, GuardDuty es un servicio regional. Las cuentas de administrador delegado de GuardDuty y sus cuentas de miembro se deben agregar a través de AWS Organizations en cada región deseada donde tenga GuardDuty habilitado. Si la cuenta de administración de la organización designa una cuenta de administrador de GuardDuty delegada solo en EE. UU. Este (Norte de Virginia), entonces la cuenta de administrador delegado de GuardDuty solo administrará cuentas de miembro agregadas a la organización en esa Región. Para obtener más información sobre la paridad de características en las regiones en las que GuardDuty se encuentra disponible, consulte [Regiones y puntos de conexión](#).

Casos especiales para las regiones incluidas

- Cuando una cuenta de administrador delegado de GuardDuty se excluye de una región incluida, aunque la organización tenga la configuración de habilitación automática de GuardDuty establecida únicamente para nuevas cuentas de miembro (NEW) o para todas las cuentas de miembro (ALL), GuardDuty no se podrá habilitar para ninguna cuenta de miembro de la organización en la que GuardDuty se encuentre desactivado en ese momento. Para obtener información sobre la configuración de sus cuentas de miembro, abra Cuentas en el panel de navegación de la [consola de GuardDuty](#) o utilice la API [ListMembers](#).
- Al utilizar la configuración de habilitación automática de GuardDuty en NEW, asegúrese de que se cumpla la siguiente secuencia:
 1. Las cuentas de miembro se incluyen en una región incluida.
 2. Agregue las cuentas de miembro a la organización en AWS Organizations.

Si cambia el orden de estos pasos, la configuración de habilitación automática de GuardDuty con NEW no funcionará en la región incluida específica porque la cuenta del miembro ya no es nueva en la organización. GuardDuty ofrece dos soluciones alternativas:

- Establezca la configuración de habilitación automática de GuardDuty en ALL, lo que incluye cuentas de miembro nuevas y existentes. En este caso, el orden de estos pasos no es relevante.
- Si una cuenta de miembro ya forma parte de la organización, administre la configuración de GuardDuty de esta cuenta individualmente en la región incluida específica. Para ello, utilice la consola de GuardDuty o la API.

Se requiere para que una organización de AWS tenga la misma cuenta de administrador delegado de GuardDuty en todas las Regiones de AWS.

Debe designar una cuenta de miembro como cuenta de administrador delegado de GuardDuty en todas las Regiones de AWS en las que GuardDuty esté habilitado. Por ejemplo, si designa una cuenta de miembro **111122223333** en **Europa (Irlanda)**, no podrá designar otra cuenta de miembro **555555555555** en **Canadá (Central)**. Se requiere que use la misma cuenta como administrador delegado de GuardDuty en todas las demás regiones.

Puede designar una nueva cuenta de administrador delegado de GuardDuty en cualquier momento. Para obtener más información sobre cómo eliminar la cuenta de administrador delegado de GuardDuty existente, consulte [Cambiar la cuenta de administrador delegado de GuardDuty](#).

No se recomienda establecer la cuenta de administración de la organización como cuenta de administrador delegado de GuardDuty.

La cuenta de administración de la organización puede ser la cuenta de administrador delegada de GuardDuty. Sin embargo, las prácticas recomendadas de seguridad de AWS siguen el principio de privilegios mínimos y no recomiendan esta configuración.

Al cambiar una cuenta de administrador delegado de GuardDuty no se desactivará GuardDuty para las cuentas de miembro.

Si quita una cuenta de administrador delegado de GuardDuty, GuardDuty quitará todas las cuentas de miembro asociadas a esta cuenta de administrador delegado de GuardDuty. GuardDuty sigue activado para todas estas cuentas de miembro.

Permisos necesarios para designar una cuenta de administrador delegado de GuardDuty

Para comenzar a utilizar Amazon GuardDuty con AWS Organizations, la cuenta de administración AWS Organizations de la organización designa una cuenta como cuenta de administrador delegado de GuardDuty. De este modo, GuardDuty se habilita como servicio de confianza en AWS Organizations. Además, habilita GuardDuty para la cuenta de administrador delegado de GuardDuty y también permite que la cuenta de administrador delegado habilite y administre GuardDuty para otras cuentas de la organización en la región actual. Para obtener información sobre cómo se conceden estos permisos, consulte [Utilizar AWS Organizations con otros servicios de AWS](#).

Como cuenta de administración de AWS Organizations, antes de designar la cuenta de administrador delegado de GuardDuty de la organización, verifique que puede realizar la siguiente acción de GuardDuty: `guardduty:EnableOrganizationAdminAccount`. Esta acción permite designar la cuenta de administrador delegado de GuardDuty de la organización mediante GuardDuty. Además, debe asegurarse de que está autorizado a realizar las acciones AWS Organizations que le ayuden a recuperar información sobre la organización.

Para conceder estos permisos, incluya la siguiente instrucción en la política (de IAM) AWS Identity and Access Management de su cuenta:

```
{
  "Sid": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}
```

Si desea designar la cuenta de administración de AWS Organizations como la cuenta de administrador delegado de GuardDuty, la cuenta también necesitará la acción de IAM: `CreateServiceLinkedRole`. Esta acción permite inicializar GuardDuty para la cuenta de administración. Sin embargo, revise [Consideraciones y recomendaciones para utilizar GuardDuty con AWS Organizations](#) antes de proceder a agregar los permisos.

Para continuar con la designación de la cuenta de administración como la cuenta de administrador delegado de GuardDuty, agregue la siguiente instrucción a la política de IAM y reemplace **111122223333** con el ID de Cuenta de AWS de la cuenta de administración de la organización:

```
{
  "Sid": "PermissionsToEnableGuardDuty"
  "Effect": "Allow",
  "Action": [
```

```
"iam:CreateServiceLinkedRole"
],
"Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
"Condition": {
  "StringLike": {
    "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
}
}
```

Designar una cuenta de administrador delegado de GuardDuty

En esta sección se indican los pasos para designar un administrador delegado en la organización de GuardDuty.

Como cuenta de administración de la organización de AWS, asegúrese de leer [Recomendaciones y consideraciones](#) sobre cómo funciona una cuenta de administrador delegado de GuardDuty. Antes de continuar, asegúrese de contar con [Permisos necesarios para designar una cuenta de administrador delegado de GuardDuty](#).

Elija un método de acceso preferente para designar una cuenta de administrador delegado de GuardDuty para la organización. Solo una cuenta de administración puede realizar este paso.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administración de la organización de AWS Organizations.

2. Con el selector Región de AWS, que aparece en la esquina superior derecha de la página, seleccione la región en la que desea designar la cuenta de administrador delegado de GuardDuty correspondiente a la organización.
3. Realice una de las siguientes acciones, en función de si GuardDuty está habilitado para la cuenta de administración en la región actual:
 - Si GuardDuty no está habilitado, seleccione Amazon GuardDuty: todas las características y elija Comenzar. Esta acción conduce a la página Bienvenido a GuardDuty.
 - Si GuardDuty está habilitado, elija Configuración en el panel de navegación.

4. En Administrador delegado, ingrese el ID de Cuenta de AWS de 12 dígitos de la cuenta que desea designar como cuenta de administrador delegado de GuardDuty para la organización.

Asegúrese de habilitar GuardDuty para la cuenta de administrador delegado de GuardDuty recién designada. De lo contrario, no podrá realizar ninguna acción.

5. Elija Delegar.
6. (Opción recomendada) Repita los pasos anteriores para designar la cuenta de administrador delegado de GuardDuty en cada región de Región de AWS en la que tenga GuardDuty habilitado.

API/CLI

1. Ejecute [enableOrganizationAdminAccount](#) con las credenciales de la Cuenta de AWS de administración de la organización.
 - También puede utilizar la AWS Command Line Interface para hacerlo. El siguiente comando de la AWS CLI designa una cuenta de administrador delegado de GuardDuty únicamente para la región actual. Ejecute el siguiente comando de la AWS CLI y asegúrese de sustituir **111111111111** por el ID de Cuenta de AWS de la cuenta que desea designar como cuenta de administrador delegado de GuardDuty:

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

Para designar la cuenta de administrador delegado de GuardDuty para otras regiones, especifique la región en el comando de la AWS CLI. En el siguiente ejemplo, se muestra cómo habilitar una cuenta de administrador delegado de GuardDuty en Oeste de EE. UU. (Oregón). Asegúrese de sustituir **us-west-2** por la región a la que desea asignar la cuenta de administrador delegado de GuardDuty.

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

Para obtener información sobre las Regiones de AWS en las que GuardDuty está disponible, consulte [Regiones y puntos de conexión](#).

Si GuardDuty está deshabilitado para la cuenta del administrador delegado de GuardDuty, no podrá realizar ninguna acción. Si aún no lo ha hecho, asegúrese de habilitar GuardDuty para la cuenta de administrador delegado de GuardDuty recién designada.

2. (Opción recomendada) repita los pasos anteriores para designar la cuenta de administrador delegado de GuardDuty en cada región de Región de AWS en la que tenga GuardDuty habilitado.

Configuración de las preferencias de habilitación automática de la organización

La característica de habilitación automática de la organización en GuardDuty ayuda a establecer el mismo estado de GuardDuty y planes de protección para ALL las cuentas de miembro existentes o NEW en la organización, en un solo paso. Del mismo modo, también puede especificar cuándo no desea realizar ninguna acción en las cuentas de miembro. Para ello, seleccione NONE. En los siguientes pasos se explica esta configuración y también se indica cuándo conviene utilizar un ajuste específico.

Note

Puede configurar las preferencias de activación automática para todos los planes de protección excepto [Protección contra malware para S3](#).

Elija un método de acceso preferente para actualizar las preferencias de habilitación automática de la organización.

Console

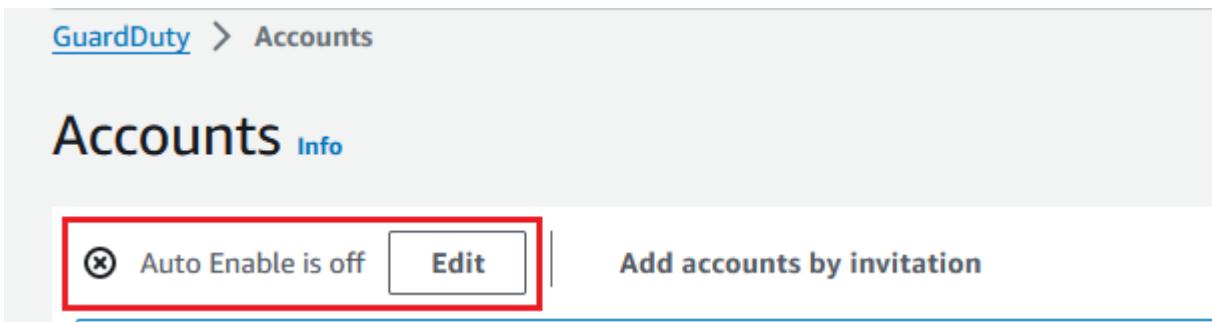
1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administrador de GuardDuty.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas se ofrecen opciones de configuración a la cuenta de administrador de GuardDuty para habilitar automáticamente GuardDuty y los planes de protección opcionales en nombre de las cuentas de miembro que pertenecen a la organización.

3. Para actualizar la configuración de habilitación automática existente, seleccione Editar.



Este soporte está disponible para configurar GuardDuty y todos los planes de protección opcionales admitidos en la Región de AWS. Puede seleccionar una de las siguientes opciones de configuración para GuardDuty en nombre de sus cuentas de miembro:

- Habilitar para todas las cuentas (**ALL**): seleccione esta opción para habilitar la opción correspondiente para todas las cuentas de una organización. Esto incluye las cuentas nuevas que se unen a la organización y las cuentas que pueden haber sido suspendidas o eliminadas de la organización. Esto también incluye la cuenta de administrador delegado de GuardDuty.

Note

Es posible que la actualización de la configuración de todas las cuentas de miembro tarde hasta 24 horas.

- Habilitar automáticamente en cuentas nuevas (**NEW**): seleccione esta opción para habilitar GuardDuty o los planes de protección opcionales únicamente en cuentas de miembro nuevas de forma automática cuando se unan a la organización.
- No habilitar (**NONE**): seleccione esta opción para impedir que se habilite la opción correspondiente en las cuentas de su organización. En este caso, la cuenta de administrador de GuardDuty administrará cada cuenta individualmente.

Al actualizar la configuración de habilitación automática de ALL o NEW a NONE, esta acción no desactiva la opción correspondiente para las cuentas existentes. Esta configuración se aplicará a las nuevas cuentas que se unan a la organización. Después de actualizar la configuración de habilitación automática, ninguna cuenta nueva tendrá la opción correspondiente como habilitada.

 Note

Cuando una cuenta de administrador delegado de GuardDuty se excluye de una región incluida, aunque la organización tenga la configuración de habilitación automática de GuardDuty establecida únicamente para nuevas cuentas de miembro (NEW) o para todas las cuentas de miembro (ALL), GuardDuty no se podrá habilitar para ninguna cuenta de miembro de la organización en la que GuardDuty se encuentre desactivado en ese momento. Para obtener información sobre la configuración de sus cuentas de miembro, abra Cuentas en el panel de navegación de la [consola de GuardDuty](#) o utilice la API [ListMembers](#).

4. Seleccione Save changes (Guardar cambios).
5. (Opcional) si desea utilizar las mismas preferencias en cada región, actualice las preferencias en cada una de las regiones admitidas por separado.

Es posible que algunos de los planes de protección opcionales no estén disponibles en todas las Regiones de AWS en las que GuardDuty está disponible. Para obtener más información, consulte [Regiones y puntos de conexión](#).

API/CLI

1. Ejecute [UpdateOrganizationConfiguration](#). Para ello, utilice las credenciales de la cuenta de administrador delegado de GuardDuty, para configurar automáticamente GuardDuty y los planes de protección opcionales en esa región para la organización. Para obtener información sobre las distintas configuraciones de habilitación automática, consulte [autoEnableOrganizationMembers](#).

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Para configurar las preferencias de habilitación automática para cualquiera de los planes de protección opcionales admitidos en su región, siga los pasos que se indican en las secciones de la documentación correspondientes a cada plan de protección.

2. Puede validar las preferencias de su organización en la región actual. Ejecuta [describeOrganizationConfiguration](#). Asegúrese de especificar el ID de detector de la cuenta de administrador delegado de GuardDuty.

 Note

La actualización de la configuración de todas las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

3. También puede ejecutar el siguiente comando de la AWS CLI para configurar las preferencias y activar o desactivar GuardDuty automáticamente en esa región para las nuevas cuentas (NEW) que se unan a la organización, todas las cuentas (ALL) o ninguna de las cuentas (NONE) de la organización. Para obtener más información, consulte [autoEnableOrganizationMembers](#). Según sus preferencias, es posible que deba sustituir NEW por ALL o NONE. Si configura el plan de protección con ALL, este también se habilitará para la cuenta del administrador delegado de GuardDuty. Asegúrese de especificar el ID de detector de la cuenta de administrador delegado de GuardDuty que administra la configuración de la organización.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

4. Puede validar las preferencias de su organización en la región actual. Ejecute el siguiente comando de la AWS CLI. Para ello, utilice el ID de detector de la cuenta de administrador delegado de GuardDuty.

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```

(Recomendado) repita los pasos anteriores en cada región. Para ello, utilice el ID de detector de la cuenta de administrador delegado de GuardDuty.

 Note

Cuando una cuenta de administrador delegado de GuardDuty se excluye de una región incluida, aunque la organización tenga la configuración de habilitación automática de GuardDuty establecida únicamente para nuevas cuentas de miembro (NEW) o para todas las cuentas de miembro (ALL), GuardDuty no se podrá habilitar para ninguna cuenta de miembro de la organización en la que GuardDuty se encuentre desactivado en ese momento. Para obtener información sobre la configuración de sus cuentas de miembro, abra Cuentas en el panel de navegación de la [consola de GuardDuty](#) o utilice la API [ListMembers](#).

Cómo agregar miembros a la organización

Como cuenta de administrador delegado de GuardDuty, puede agregar una o más Cuentas de AWS a la organización de GuardDuty. Cuando agregue una cuenta como miembro de GuardDuty, el servicio se activará automáticamente en esa región. Hay una excepción a la cuenta de administración de la organización. Antes de que la cuenta de administración se agregue como miembro de GuardDuty, debe tener GuardDuty activado.

Elija el método que prefiera para agregar una cuenta de miembro a la organización de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.

La tabla de cuentas muestra todas las cuentas de miembro que están activas (no suspendidas Cuentas de AWS) y que pueden estar asociadas a la cuenta de administrador delegado de GuardDuty. Si la cuenta de miembro está asociada a la cuenta de administrador de la organización, el Tipo será uno de los siguientes: A través de Organizations o Por invitación. Si una cuenta de miembro no está asociada a la cuenta de administrador de GuardDuty de la organización, el Tipo de esta cuenta de miembro es No es miembro.

3. Seleccione uno o varios ID de cuenta que desee agregar en calidad de miembros. Estos ID de cuenta deben tener el Tipo como A través de organizaciones.

Las cuentas que se agregan por invitación no forman parte de su organización. Puede administrador dichas cuentas de forma individual. Para obtener más información, consulte [Administración de cuentas por invitación](#).

4. Seleccione el menú desplegable Acciones y, a continuación, elija Agregar miembro. Después de agregar esta cuenta como miembro, se aplicará la configuración de habilitación automática de GuardDuty. Según los ajustes de [Configuración de las preferencias de habilitación automática de la organización](#), la configuración de GuardDuty de estas cuentas puede cambiar.
5. Puede seleccionar la flecha hacia abajo de la columna Estado para ordenar las cuentas según el estado No es miembro y, a continuación, elegir cada cuenta que no tenga GuardDuty habilitado en la región actual.

Si ninguna de las cuentas que figuran en la tabla de cuentas se ha agregado todavía como miembro, puede habilitar GuardDuty en la región actual para todas las cuentas de la organización. Elija Habilitar en el encabezado de la parte superior de la página. Esta acción activa automáticamente la configuración Habilitar automáticamente para que GuardDuty se habilite en cualquier cuenta nueva que se una a la organización.

6. Elija Confirmar para agregar las cuentas como miembros. Esta acción también habilita GuardDuty para todas las cuentas seleccionadas. El Estado de las cuentas invitadas cambiará a Habilitado.
7. (Recomendado) Repita estos pasos en cada Región de AWS. Esto garantiza que la cuenta de administrador delegado de GuardDuty pueda administrar los resultados y otras configuraciones de las cuentas de miembro en todas las regiones en las que GuardDuty esté habilitado.

La característica de habilitación automática activa GuardDuty para todos los futuros miembros de su organización. Esto permite que la cuenta de administrador delegada de GuardDuty administre cualquier miembro nuevo que se cree dentro de la organización o se agregue a esta. Cuando la cantidad de cuentas de miembro alcanza el límite de 50 000, la característica de habilitación automática se desactiva automáticamente. Si se elimina una cuenta de miembro y la cantidad total de miembros disminuye por debajo de 50 000, la característica de habilitación automática se activa de nuevo.

API/CLI

- Ejecute [CreateMembers](#). Para ello, utilice las credenciales de la cuenta de administrador delegado de GuardDuty.

Debe especificar el ID de detector regional de la cuenta de administrador delegado de GuardDuty y los detalles de la cuenta (ID de la Cuenta de AWS y direcciones de correo electrónico correspondientes) de las cuentas que desea agregar como miembros de GuardDuty. Puede crear uno o varios miembros con esta operación de API.

Cuando ejecute CreateMembers en la organización, las preferencias de habilitación automática para nuevos miembros se aplicarán a medida que nuevas cuentas de miembro se unan a la organización. Cuando se ejecuta CreateMembers con una cuenta de miembro existente, la configuración de la organización también se aplicará a los miembros existentes. Esto podría cambiar la configuración actual de las cuentas de miembro existentes.

Ejecute [ListAccounts](#) en la referencia de la API de AWS Organizations. De este modo, podrá ver todas las cuentas de la organización de AWS.

- Como alternativa también puede utilizar la AWS Command Line Interface. Ejecute el siguiente comando de la AWS CLI y asegúrese de utilizar su propio ID de detector válido, su ID de Cuenta de AWS y la dirección de correo electrónico asociada al ID de la cuenta.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--account-details AccountId=111122223333,Email=guardduty-member-  
name@amazon.com
```

Para ver una lista de todos los miembros de la organización, ejecute el siguiente comando de la AWS CLI:

```
aws organizations list-accounts
```

Después de agregar esta cuenta como miembro, se aplicará la configuración de habilitación automática de GuardDuty.

(Opcional) Habilitar planes de protección para cuentas de miembro existentes

El siguiente procedimiento incluye los pasos para habilitar planes de protección para cuentas de miembro existentes mediante la página Cuentas. Para conocer los pasos que hay que seguir para ello a través de la API o la AWS CLI, consulte los documentos relacionados con el plan de protección específico.

Puede habilitar planes de protección para cuentas individuales a través de la página Cuentas.

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Utilice las credenciales de cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.
3. Seleccione una o más cuentas donde desee configurar un plan de protección. Repita los pasos siguientes para cada plan de protección que desee configurar:
 - a. Seleccione Editar planes de protección.
 - b. En la lista de planes de protección, elija aquel que desee configurar.
 - c. Elija una de las acciones que desee llevar a cabo para este plan de protección y, a continuación, seleccione Confirmar.
 - d. Para la cuenta seleccionada, la columna correspondiente al plan de protección configurado mostrará la configuración actualizada como Habilitado o No habilitado.

Administración continua de las cuentas de miembro en GuardDuty

Como cuenta de administrador delegado de GuardDuty, es responsable de mantener la configuración de GuardDuty y sus planes de protección opcionales para todas las cuentas de la organización en cada Región de AWS admitida. En las siguientes secciones se ofrecen las opciones sobre cómo mantener el estado de configuración de GuardDuty o de cualquiera de sus planes de protección opcionales:

Para mantener el estado de configuración de toda la organización en cada región

- Configure las preferencias de habilitación automática para toda la organización mediante la consola de GuardDuty: puede habilitar GuardDuty automáticamente para todos (ALL) los miembros de la organización o para los nuevos (NEW) miembros que se unan a la organización,

u optar por no (NONE) habilitar el servicio automáticamente para ninguno de los miembros de la organización.

También puede configurar la misma configuración o una diferente para cualquiera de los planes de protección dentro de GuardDuty.

Es posible que la actualización de la configuración de todas las cuentas de miembro de la organización tarde hasta 24 horas.

- Actualice las preferencias de habilitación automática mediante la API: ejecute [UpdateOrganizationConfiguration](#) para configurar automáticamente GuardDuty y sus planes de protección opcionales para la organización. Cuando ejecute [CreateMembers](#) para agregar nuevas cuentas de miembro en la organización, los ajustes configurados se aplicarán automáticamente. Cuando se ejecuta CreateMembers con una cuenta de miembro existente, la configuración de la organización también se aplicará a los miembros existentes. Esto podría cambiar la configuración actual de las cuentas de miembro existentes.

Para ver todas las cuentas de la organización, ejecute [ListAccounts](#) en la referencia de la API AWS Organizations.

Para mantener el estado de configuración de las cuentas de miembro individualmente en cada región

- Para ver todas las cuentas de la organización, ejecute [ListAccounts](#) en la referencia de la API AWS Organizations.
- Si desea que algunas cuentas de miembro tengan un estado de configuración diferente, ejecute [UpdateMemberDetectors](#) para cada cuenta de miembro individualmente.

Puede utilizar la consola de GuardDuty para realizar la misma tarea. Para ello, vaya a la página Cuentas de la consola de GuardDuty.

Para obtener información sobre cómo habilitar planes de protección para cuentas individuales ya sea mediante la consola o la API, consulte la página de configuración del plan de protección correspondiente.

Suspender GuardDuty para la cuenta de miembro

Como cuenta de administrador delegado de GuardDuty, puede suspender el servicio de GuardDuty para una cuenta de miembro en la organización. Si hace esto, la cuenta de miembro permanece en la organización de GuardDuty. También podrá volver a habilitar GuardDuty para estas cuentas

de miembro más adelante. Sin embargo, si finalmente desea desasociar (eliminar) esta cuenta de miembro, después de seguir los pasos que se indican en esta sección, deberá seguir los pasos que se indican en [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#).

Al suspender GuardDuty en una cuenta de miembro, se pueden prever los siguientes cambios:

- GuardDuty ya no supervisa la seguridad del entorno de AWS ni genera nuevos resultados.
- Los resultados existentes en la cuenta de miembro permanecen intactos.
- Una cuenta de miembro suspendida por GuardDuty no incurre en ningún cargo por GuardDuty.

Si la cuenta de miembro ha habilitado la protección contra malware para S3 para uno o más buckets en la cuenta, suspender GuardDuty no afectará a la configuración de la protección contra malware para S3. La cuenta de miembro aún incurrirá en el costo de uso correspondiente a la protección contra malware para S3. Para que la cuenta de miembro deje de utilizar la protección contra malware para S3, se debe desactivar esta característica para los buckets protegidos. Para obtener más información, consulte [Desactivar la protección contra malware para S3 para un bucket protegido](#).

Elija un método preferente para suspender GuardDuty en una cuenta de miembro de la organización.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.
3. En la página Cuentas, seleccione una o más cuentas para las que desee suspender GuardDuty.
4. Elija el menú desplegable Acciones y, a continuación, elija Suspender GuardDuty.
5. Seleccione Suspender GuardDuty para confirmar la opción seleccionada.

Esto cambiará el Estado de la cuenta de miembro a Desactivado (suspendido).

Repita los pasos anteriores en cada región adicional en la que desee desasociar o eliminar la cuenta de miembro.

API

1. Para recuperar el ID de la cuenta de miembro para la que desea suspender GuardDuty, utilice la API [ListMembers](#). Incluya el parámetro `OnlyAssociated` en la solicitud. Si establece el valor de este parámetro en `true`, GuardDuty devuelve una matriz `members` que brinda detalles sobre únicamente aquellas cuentas que actualmente son miembros de GuardDuty.

Otra posibilidad es utilizar AWS Command Line Interface (AWS CLI) para ejecutar el siguiente comando:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Sustituya *us-east-1* por la región en la que desea suspender GuardDuty para esta cuenta.

2. Para suspender una o más cuentas de miembro de GuardDuty, ejecute [StopMonitoringMembers](#) para suspender GuardDuty para una cuenta de miembro.

Otra posibilidad es utilizar AWS CLI para ejecutar el siguiente comando:

```
aws guardduty stop-monitoring-members --detector-id  
12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Sustituya *us-east-1* por la región en la que desea suspender esta cuenta. Si tiene una lista de identificadores de cuenta que desea eliminar, sepárelos con un espacio.

Si además desea desasociar (eliminar) esta cuenta de miembro, siga los pasos que se indican en [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#).

Desasociar (eliminar) la cuenta de miembro de la cuenta de administrador

Cuando desee dejar de configurar los ajustes de GuardDuty y de acceder a los datos desde una cuenta de miembro, elimine esa cuenta como cuenta de miembro de GuardDuty. Para ello, desasocie (elimine) esa cuenta de la cuenta de administrador de GuardDuty.

Al desvincular una cuenta de miembro de GuardDuty, se producirá lo siguiente:

- GuardDuty permanecerá habilitado para la cuenta en la Región de AWS actual, pero la cuenta se desvinculará de la cuenta de administrador delegado de GuardDuty.

- La cuenta desvinculada aún aparece en el inventario de cuentas.
- La cuenta de administrador de GuardDuty ya no tiene acceso a los resultados de esta cuenta independiente.
- El propietario de la cuenta no recibe ninguna notificación de la desvinculación.

Puede volver a agregar la cuenta desvinculada a la organización en un momento posterior.

Elija el método que prefiera para desasociar (eliminar) una cuenta de miembro de la organización.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.
3. En la tabla Cuentas, puede eliminar una cuenta que tenga Tipo como Vía Organizations y Estado como Habilitado.

Seleccione una o más cuentas que tengan el mismo Tipo y Estado.

4. En el menú desplegable Acciones, seleccione Desasociar cuenta.
5. Elija Desasociar cuenta para confirmar la opción elegida.
6. El valor de Estado de las cuentas seleccionadas cambiará a No es miembro. El recuento de Vía Organizations (Activas/Todas) que aparece en la esquina superior derecha de la página Cuentas cambiará de modo que se refleje la actualización.

Repita los pasos descritos anteriormente en cada región adicional en la que desee desasociar la cuenta de miembro.

API

1. Para recuperar el ID de cuenta de la cuenta de miembro que desea eliminar, utilice la API [ListMembers](#). Incluya el parámetro `OnlyAssociated` en la solicitud. Si establece el valor de este parámetro en `true`, GuardDuty devuelve una matriz `members` que brinda detalles sobre únicamente aquellas cuentas que actualmente son miembros de GuardDuty.

Otra posibilidad es utilizar AWS Command Line Interface (AWS CLI) para ejecutar el siguiente comando:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Sustituya *us-east-1* por la región en la que desea eliminar esta cuenta.

2. Para eliminar una o más cuentas de miembro de GuardDuty, ejecute [DisassociateMembers](#) para eliminar la cuenta de miembro asociada a la cuenta de administrador.

Otra posibilidad es utilizar AWS CLI para ejecutar el siguiente comando:

```
aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE  
--account-ids 111122223333 --region us-east-1
```

Sustituya *us-east-1* por la región en la que desea eliminar esta cuenta. Si tiene una lista de identificadores de cuenta que desea eliminar, sepárelos con un espacio.

Eliminar cuentas de miembro de la organización de GuardDuty

Como cuenta de administrador delegado de GuardDuty, después de que haya desasociado una cuenta de miembro y ya no desee mantener esa cuenta de miembro en la organización de GuardDuty, podrá eliminar la cuenta de miembro de la organización de GuardDuty. Esta cuenta de miembro dejará de aparecer en el inventario de cuentas. Sin embargo, si GuardDuty no se suspendió en esta cuenta de miembro, la configuración de GuardDuty y los planes de protección dedicada se mantienen iguales. Esta cuenta pasará a ser una cuenta independiente y podrá [deshabilitar GuardDuty](#) por sí misma.

Este paso no eliminará la cuenta de miembro de la organización de AWS.

Elija el método que prefiera para eliminar una cuenta de miembro de la organización de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administrador delegado de GuardDuty.

2. En el panel de navegación, elija Cuentas.

3. En la tabla Cuentas, puede eliminar una cuenta que tenga Tipo como Vía Organizations y Estado como Eliminada (desasociada).

Seleccione una o más cuentas que tengan el mismo Tipo y Estado.

4. En el menú desplegable Acciones, elija Eliminar cuenta.
5. Elija Eliminar cuentas para confirmar la opción elegida. La cuenta de miembro seleccionada ya no aparecerá en la tabla Cuentas.

Repita los pasos descritos anteriormente en cada región adicional en la que desee eliminar esta cuenta de miembro.

API/CLI

1. Para recuperar el ID de cuenta de la cuenta de miembro que desea eliminar, utilice la API [ListMembers](#). Incluya el parámetro `OnlyAssociated` en la solicitud. Si establece el valor de este parámetro en `false`, GuardDuty devuelve una matriz `members` que brinda detalles sobre únicamente aquellas cuentas que actualmente son miembros desasociados de GuardDuty.

Otra posibilidad es utilizar AWS Command Line Interface (AWS CLI) para ejecutar el siguiente comando:

```
aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
```

Sustituya `12abc34d567e8fa901bc2d34EXAMPLE` por el ID de detector de cuenta de administrador delegado de GuardDuty y `us-east-1` por la región en la que desea eliminar la cuenta.

2. Para eliminar una o más cuentas de miembro de GuardDuty, ejecute [DeleteMembers](#) para eliminar la cuenta de miembro de la organización de GuardDuty.

Otra posibilidad es utilizar AWS CLI para ejecutar el siguiente comando:

```
aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Sustituya `12abc34d567e8fa901bc2d34EXAMPLE` por el ID de detector de cuenta de administrador delegado de GuardDuty y `us-east-1` por la región en la que desea eliminar la

cuenta. Si tiene una lista de identificadores de cuenta que desea eliminar, sepárelos con un espacio.

Cambiar la cuenta de administrador delegado de GuardDuty

Puede eliminar la cuenta de administrador delegado de GuardDuty para la organización en cada región y luego delegar un nuevo administrador en cada región. Para mantener la postura de seguridad de las cuentas de miembro de la organización en una región, debe tener una cuenta de administrador delegado de GuardDuty en esa región.

Nota

Antes de eliminar una cuenta de administrador delegado de GuardDuty, debe desasociar todas las cuentas de miembro asociadas a la cuenta de administrador delegado de GuardDuty, y posteriormente eliminarlas de la organización de GuardDuty. Para obtener más información sobre estos pasos, consulte los siguientes documentos:

- [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#)
- [Eliminar cuentas de miembro de la organización de GuardDuty](#)

Eliminar una cuenta de administrador delegado de GuardDuty existente

Paso 1: Para eliminar la cuenta de administrador delegado de GuardDuty existente en cada región

1. Como cuenta de administrador delegado de GuardDuty existente, enumere todas las cuentas de miembro asociadas a la cuenta de administrador. Ejecutar [ListMembers](#) con `OnlyAssociated=false`.
2. Si la preferencia de habilitación automática para GuardDuty o cualquiera de los planes de protección opcionales está establecida en ALL, entonces ejecute [UpdateOrganizationConfiguration](#) para actualizar la configuración de la organización a NEW o NONE. Esta acción evitará que se produzca un error al desasociar todas las cuentas de miembro en el paso siguiente.
3. Ejecute [DisassociateMembers](#) para desasociar todas las cuentas de miembro que están asociadas a la cuenta de administrador.
4. Ejecute [DeleteMembers](#) para eliminar las asociaciones entre la cuenta de administrador y las cuentas de miembro.

5. Como cuenta de administración de la organización, ejecute [DisableOrganizationAdminAccount](#) para eliminar la cuenta existente de administrador delegado de GuardDuty.
6. Repita estos pasos en cada Región de AWS en la que tenga esta cuenta de administrador delegado de GuardDuty.

Paso 2: para anular el registro de una cuenta de administrador delegado de GuardDuty existente en AWS Organizations (acción global única)

- Ejecute [DeregisterDelegatedAdministrator](#) en la referencia de la API AWS Organizations, para anular el registro de la cuenta de administrador delegado de GuardDuty existente en AWS Organizations.

También puede ejecutar el siguiente comando de la AWS CLI:

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --  
service-principal guardduty.amazonaws.com
```

Asegúrese de sustituir **111122223333** por la cuenta de administrador delegado de GuardDuty existente.

Después de anular el registro de la antigua cuenta de administrador delegado de GuardDuty, puede agregarla como cuenta de miembro a la nueva cuenta de administrador delegado de GuardDuty.

Designar una nueva cuenta de administrador delegado de GuardDuty en cada región

1. Designe una nueva cuenta de administrador delegado de GuardDuty en cada región por medio del método de acceso que prefiera: consola de GuardDuty, o la API o la AWS CLI. Para obtener más información, consulte [Designar una cuenta de administrador delegado de GuardDuty](#).
2. Ejecute [DescribeOrganizationConfiguration](#) para ver la configuración actual de habilitación automática de la organización.

Important

Antes de agregar cualquier miembro a la nueva cuenta de administrador delegado de GuardDuty, debe verificar la configuración de habilitación automática de la organización. Esta configuración se aplica específicamente a la nueva cuenta de administrador

delegado de GuardDuty y a la región seleccionada, y no se relaciona con AWS Organizations. Cuando se agrega (nueva o existente) una cuenta de miembro de organización bajo la nueva cuenta de administrador delegado de GuardDuty, la configuración de habilitación automática de la nueva cuenta de administrador delegado de GuardDuty se aplicará al momento de habilitar GuardDuty o cualquiera de sus planes de protección opcionales.

Cambia la configuración de la organización para la nueva cuenta de administrador delegado de GuardDuty a través del método de acceso que prefiera: consola de GuardDuty, o la API o la AWS CLI. Para obtener más información, consulte [Configuración de las preferencias de habilitación automática de la organización](#).

Administración de cuentas de GuardDuty por invitación

Para administrar cuentas que estén fuera de la organización, puede utilizar el método de invitación heredado. Con este método, su cuenta se designa como cuenta de administrador cuando otra cuenta acepta su invitación para convertirse en cuenta de miembro.

Note

GuardDuty recomienda utilizar AWS Organizations en lugar de las invitaciones de GuardDuty para administrar las cuentas de miembro. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Si la cuenta no es de administrador, podrá aceptar una invitación de otra cuenta. Al aceptar, su cuenta se convierte en cuenta miembro. Una cuenta de AWS no puede ser una cuenta de administrador de y una cuenta de miembro de GuardDuty a la vez.

Si acepta una invitación de una cuenta, no podrá aceptar una invitación de otra cuenta. Para aceptar una invitación de otra cuenta, primero tendrá que desasociar su cuenta de la cuenta de administrador existente. Como alternativa, la cuenta de administrador también puede desasociar la cuenta y eliminarla de su organización.

Las cuentas que se asocian a través de una invitación tienen una relación de cuenta de administrador y miembro similar a las cuentas asociadas mediante AWS Organizations, tal y como se describe en [Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas](#)

[de miembro](#). Sin embargo, los usuarios de la cuenta de administrador que utilizan invitaciones no pueden habilitar GuardDuty en nombre de las cuentas de miembro asociadas ni ver otras cuentas de la organización de AWS Organizations que no sean de miembro.

 Important

Cuando GuardDuty crea cuentas de miembro con este método, pueden transferirse datos entre regiones. Para verificar las direcciones de correo electrónico de las cuentas de miembro, GuardDuty utiliza un servicio de verificación de correo electrónico que solo funciona en la región Este de EE. UU. (Norte de Virginia).

Temas

- [Agregar cuentas por invitación](#)
- [Consolidación de cuentas de administrador de GuardDuty bajo una sola organización](#)

Agregar cuentas por invitación

Como cuenta de administrador con GuardDuty habilitado, podrá agregar miembros de modo que comiencen a utilizar GuardDuty. Tras agregar a los miembros, podrá invitarlos a que se unan a GuardDuty. Por su parte, ellos decidirán si responden a la invitación.

 Note

GuardDuty recomienda utilizar AWS Organizations en lugar de las invitaciones de GuardDuty para administrar las cuentas de miembro. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Elija un método de acceso preferente para agregar cuentas de miembro de GuardDuty como cuenta de administrador de GuardDuty.

Console

Paso 1: agregación de una cuenta

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Cuentas.

3. Seleccione Agregar cuentas mediante invitación en el panel superior.
4. En la página Agregar cuentas de miembros, en Escribir los detalles de la cuenta, introduzca el ID de la Cuenta de AWS y la dirección de correo electrónico asociada a la cuenta que desea agregar.
5. Para agregar otra fila para introducir los detalles de la cuenta de uno en uno, elija Agregar otra cuenta. También puede seleccionar Cargar un archivo .csv con los detalles de la cuenta para agregar cuentas en bloque.

 Important

La primera línea del archivo .csv debe contener el encabezado, tal como se muestra en el ejemplo siguiente: `. – Account ID,Email`. Cada línea subsiguiente debe contener un único ID de Cuenta de AWS válido y su dirección de correo electrónico asociada. El formato de una fila es válido si contiene solo un ID de Cuenta de AWS y la dirección de correo electrónico asociada separados por una coma.

```
Account ID,Email
```

```
55555555555, user@example.com
```

6. Después de agregar todos los detalles de las cuentas, seleccione Siguiente. Puede ver las cuentas recién agregadas en la tabla Cuentas. El Estado de estas cuentas será Invitación no enviada. Para obtener información sobre cómo enviar una invitación a una o más cuentas agregadas, consulte [Step 2 - Invite an account](#).

Paso 2: invitación a una cuenta

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Cuentas.
3. Seleccione una o varias cuentas que desee invitar a Amazon GuardDuty.
4. Seleccione el menú desplegable Acciones y, a continuación, elija Invitar.
5. En el cuadro de diálogo Invitación a GuardDuty, introduzca un mensaje de invitación (opcional).

Si la cuenta invitada no tiene acceso al correo electrónico, seleccione la casilla Enviar también una notificación de correo electrónico al usuario raíz de la Cuenta de AWS del invitado y generar una alerta en la AWS Health Dashboard del invitado.

6. Seleccione Send invitation (Enviar invitación). Si los invitados tienen acceso a la dirección de correo electrónico especificada, pueden abrir la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/> para ver la invitación.
7. Cuando el invitado acepta la invitación, el valor de la columna Estado cambia a Invitado. Para obtener más información sobre la aceptación de una invitación, consulte [Step 3 - Accept an invitation](#).

Paso 3: aceptación de una invitación

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Important

Debe habilitar GuardDuty antes de poder ver o aceptar una invitación para hacerse miembro.

2. Haga lo siguiente solo si aún no ha activado GuardDuty; de lo contrario, puede omitir este paso y continuar con el siguiente.

Si aún no ha activado GuardDuty, seleccione Comenzar en la página de Amazon GuardDuty.

En la página Bienvenido a GuardDuty, elija Habilitar GuardDuty.

3. Después de activar GuardDuty en su cuenta, siga estos pasos para aceptar la invitación para hacerse miembro:
 - a. En el panel de navegación, seleccione Configuración.
 - b. Elija Cuentas.
 - c. En Cuentas, asegúrese de verificar el propietario de la cuenta desde la que acepta la invitación. Active Aceptar para aceptar la invitación para hacerse miembro.
4. Después de aceptar la invitación, su cuenta se convierte en una cuenta de miembro de GuardDuty. La cuenta de cuyo propietario ha enviado la invitación se convierte en cuenta de administrador de GuardDuty. La cuenta de administrador sabrá que ha aceptado la invitación. Se actualizará la tabla Cuentas de su cuenta de GuardDuty. El valor de la columna Estado correspondiente al ID de la cuenta de miembro cambiará a Habilitado. El propietario de la cuenta de administrador ahora puede ver y administrar las configuraciones de GuardDuty y del plan de protección en nombre de su cuenta. La cuenta de administrador también puede ver y administrar los resultados de GuardDuty generados para su cuenta de miembro.

API/CLI

Puede designar una cuenta de administrador de GuardDuty y crear o agregar cuentas de miembro de GuardDuty mediante invitación a través de las operaciones de la API. Ejecute las siguientes operaciones de la API de GuardDuty para designar la cuenta de administrador y las cuentas de miembro de GuardDuty.

Complete el siguiente procedimiento con las credenciales de la Cuenta de AWS que desea designar como cuenta administradora de GuardDuty.

Creación o agregación de cuentas de miembro

1. Ejecute la operación de la API [CreateMembers](#) con las credenciales de la cuenta de AWS en la que GuardDuty está habilitado. Esta es la cuenta que desea que sea la cuenta de administrador de GuardDuty.

Debe especificar el ID de detector de la cuenta de AWS actual, así como el ID de cuenta y la dirección de correo electrónico de las cuentas que quiere convertir en miembros de GuardDuty. Puede crear uno o varios miembros con esta operación de API.

También puede utilizar las herramientas de línea de comandos de AWS para designar la cuenta de administrador. Para ello, ejecute el siguiente comando de la CLI. No olvide utilizar su propio ID de detector, ID de cuenta y correo electrónico.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Ejecute [InviteMembers](#) con las credenciales de la cuenta de AWS que tiene GuardDuty habilitado. Esta es la cuenta que desea que sea la cuenta de administrador de GuardDuty.

Debe especificar el ID de detector de la cuenta de AWS actual, así como los ID de las cuentas que quiere convertir en miembros de GuardDuty. Con esta operación de la API, puede invitar a uno o varios miembros.

 Note

También puede especificar un mensaje de invitación opcional mediante el parámetro de solicitud `message`.

También puede utilizar AWS Command Line Interface para designar las cuentas de miembro con el siguiente comando. No olvide utilizar su propio ID de detector y unos ID válidos para las cuentas a las que desea invitar.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-ids 111122223333
```

Aceptación de invitaciones

Complete el siguiente procedimiento con las credenciales de cada cuenta de AWS que desea designar como cuenta de miembro de GuardDuty.

1. Ejecute la operación de la API [CreateDetector](#) en cada cuenta de AWS a la que ha enviado una invitación para convertirse en cuenta de miembro de GuardDuty y donde desee aceptar una invitación.

Debe especificar si el recurso del detector se va a habilitar mediante el servicio de GuardDuty. Debe crearse y habilitarse un detector para que GuardDuty entre en funcionamiento. Antes de aceptar una invitación, primero debe habilitar GuardDuty.

También puede hacerlo mediante las herramientas de línea de comandos de AWS con el siguiente comando de la CLI.

```
aws guardduty create-detector --enable
```

2. Ejecute la operación de la API [AcceptAdministratorInvitation](#) en cada cuenta de AWS que desee que acepte la invitación para convertirse en cuenta de miembro mediante las credenciales de la cuenta.

Debe especificar el ID de detector de esta cuenta de AWS para la cuenta de miembro, el ID de cuenta de la cuenta de administrador que ha enviado la invitación y el ID de la invitación que va a aceptar. Puede consultar el ID de cuenta de la cuenta de administrador en el correo electrónico de invitación o con la operación [ListInvitations](#) de la API.

También puede aceptar una invitación utilizando las herramientas de línea de comandos de AWS con el siguiente comando de la CLI. No olvide utilizar un ID de detector, un ID de cuenta de administrador y un ID de invitación que sean válidos.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--administrator-id 444455556666 --invitation-  
id 84b097800250d17d1872b34c4daadc5
```

Consolidación de cuentas de administrador de GuardDuty bajo una sola organización

GuardDuty recomienda utilizar la asociación a través de AWS Organizations a fin de administrar cuentas de miembro bajo una cuenta de administrador delegado de GuardDuty. Puede emplear el proceso ejemplificado a continuación para consolidar la cuenta de administrador y la cuenta de miembro asociadas mediante invitación dentro de una organización, bajo una única cuenta de administrador delegado de GuardDuty.

Note

GuardDuty recomienda utilizar AWS Organizations en lugar de las invitaciones de GuardDuty para administrar las cuentas de miembro. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Las cuentas que ya administra una cuenta de administrador delegado de GuardDuty o las cuentas de miembro activas asociadas a una cuenta de administrador delegado de GuardDuty no se pueden agregar a una cuenta de administrador delegado de GuardDuty diferente. Cada organización solo

puede tener una cuenta de administrador delegado de GuardDuty por región y cada cuenta de miembro solo puede tener una cuenta de administrador delegado de GuardDuty.

Elija uno de los métodos de acceso preferentes para consolidar las cuentas de administrador de GuardDuty bajo una sola cuenta de administrador delegado de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administración de la organización.

2. Todas las cuentas para las que desee administrar GuardDuty deben formar parte de su organización. Para más información acerca de cómo agregar una cuenta a su organización, consulte [Invitar a una Cuenta de AWS a unirse a su organización](#).
3. Asegúrese de que todas las cuentas de miembro estén asociadas a la cuenta que desea designar como única cuenta de administrador delegado de GuardDuty. Desasocie cualquier cuenta de miembro que aún esté asociada a las cuentas de administrador preexistentes.

Los siguientes pasos le ayudarán a desasociar las cuentas de miembro de la cuenta de administrador preexistente:

- a. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
 - b. Para iniciar sesión, utilice las credenciales de la cuenta de administrador preexistente.
 - c. En el panel de navegación, elija Cuentas.
 - d. En la página Cuentas, seleccione una o más cuentas que quiera desasociar de la cuenta de administrador.
 - e. Seleccione Acciones y, a continuación, seleccione Desasociar cuenta.
 - f. Seleccione Confirmar para finalizar el paso.
4. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administración.

5. En el panel de navegación, seleccione Configuración. En la página Configuración, designe la cuenta de administrador delegado de GuardDuty para la organización.
6. Inicie sesión en la cuenta de administrador delegado de GuardDuty designada.
7. Agregue miembros de la organización. Para obtener más información, consulte [Administración de cuentas de GuardDuty con AWS Organizations](#).

API/CLI

1. Todas las cuentas para las que desee administrar GuardDuty deben formar parte de su organización. Para más información acerca de cómo agregar una cuenta a su organización, consulte [Invitar a una Cuenta de AWS a unirse a su organización](#).
2. Asegúrese de que todas las cuentas de miembro estén asociadas a la cuenta que desea designar como única cuenta de administrador delegado de GuardDuty.
 - a. Ejecute [DisassociateMembers](#) para desasociar cualquier cuenta de miembro que aún esté asociada a las cuentas de administrador preexistentes.
 - b. Como alternativa, puede utilizar AWS Command Line Interface para ejecutar el siguiente comando y sustituir **777777777777** por el ID de detector de la cuenta de administrador preexistente de la que desea desasociar la cuenta de miembro. Sustituya **666666666666** por el ID de Cuenta de AWS de la cuenta de miembro que desee desasociar.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
```

3. Ejecute [EnableOrganizationAdminAccount](#) para delegar una Cuenta de AWS como cuenta de administrador delegado de GuardDuty.

Como alternativa, puede utilizar AWS Command Line Interface para ejecutar el siguiente comando para delegar una cuenta de administrador delegado de GuardDuty:

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Agregue miembros de la organización. Para obtener más información, consulte [Create or add member member accounts using API](#).

 Important

Para maximizar la eficacia de GuardDuty, un servicio regional, recomendamos que designe la cuenta de administrador delegado de GuardDuty y agregue todas las cuentas de miembro en cada región.

Consideraciones sobre GuardDuty para exportar los detalles de las cuentas de miembro en formato CSV

Como cuenta de administrador de GuardDuty, puede exportar los detalles de la cuenta de miembro en formato CSV. Estos detalles incluyen el ID de la cuenta de miembro, nombre, tipo (agregado por AWS Organizations o a través de invitación), y estado de configuración de GuardDuty y planes de protección dedicados.

La opción Exportar CSV aparece en la página Cuentas de GuardDuty según cómo administre las múltiples cuentas de miembro. Al utilizar la opción Exportar CSV, podrá identificar qué cuentas de miembro tienen habilitado un plan de protección específico.

En la siguiente lista se indican los criterios que definen si la opción Exportar CSV se encontrará disponible o no en la página de Cuentas de GuardDuty:

- Sólo utiliza AWS Organizations para administrar múltiples cuentas de miembro y la cantidad total de cuentas de miembro en la organización GuardDuty es de hasta 5000.
- Utiliza tanto el método AWS Organizations como el de invitaciones, y la cantidad total de cuentas de miembro en la organización GuardDuty es de hasta 5000.

En este caso, el CSV exportado incluirá si una cuenta de miembro se agregó a través de AWS Organizations o mediante el método basado en invitaciones.

- Si utiliza únicamente el método basado en invitaciones para administrar varias cuentas de miembro, no existirá la opción Exportar CSV.

Tipos de resultados de GuardDuty

Un resultado es una notificación que GuardDuty genera cuando detecta un indicio de una actividad sospechosa o maliciosa en su parte Cuenta de AWS. GuardDuty genera un resultado en una cuenta que ha activado GuardDuty.

Para obtener más información acerca de cambios importantes en los tipos de resultado de GuardDuty, incluidos los retirados o añadidos recientemente, consulte [Historial de documentación de Amazon GuardDuty](#).

Para obtener información sobre tipos de resultados que ya se han retirado, consulte [Tipos de resultados retirados](#).

Tipos de resultados de EC2 en GuardDuty

Los siguientes resultados son específicos de los recursos de Amazon EC2 y siempre tendrán un tipo de recurso de Instance. La gravedad y los detalles de los resultados variarán en función del rol de recurso que indicará si la instancia de EC2 fue objeto de actividad sospechosa o el agente que llevó a cabo la actividad.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para más información sobre los orígenes de datos y modelos, consulte [Orígenes de datos fundamentales de GuardDuty](#).

Notas

- Es posible que falten detalles de la instancia de resultados de EC2 si la instancia ya se terminó o si la llamada a la API subyacente se originó en una instancia de EC2 en una región diferente.
- Los resultados de EC2 que utilizan registros de flujo de VPC como origen de datos no admiten el tráfico IPv6.

Para todos los resultados de EC2, se recomienda examinar el recurso en cuestión para determinar si se comporta de la manera esperada. Si la actividad está autorizada, puede utilizar reglas de supresión o listas de IP confiables para evitar las notificaciones de falsos positivos para ese recurso.

Si la actividad es inesperada, la práctica recomendada de seguridad consiste en asumir que la instancia se ha visto afectada y llevar a cabo las acciones detalladas en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Temas

- [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

Una instancia de EC2 está consultando una IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que hay una instancia que aparece en la lista dentro del entorno de AWS que está consultando a una IP asociada con un servidor de comando y control (C&C) conocido. La instancia de la lista podría haberse visto afectada. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de

la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

Note

Si la IP consultada está relacionada con log4j, los campos del resultado asociado incluirán los siguientes valores:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/C&CActivity.B!DNS

La instancia de EC2 está consultando un nombre de dominio que está asociado a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia que se muestra en la lista dentro del entorno de AWS que está consultando a un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La instancia de la lista podría haberse visto afectada. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

Note

Si el nombre de dominio consultado está relacionado con log4j, los campos del resultado asociado incluirán los siguientes valores:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

Note

Para probar cómo GuardDuty genera este tipo de resultado, puede hacer una solicitud de DNS desde su instancia (mediante `dig` para Linux o `nslookup` para Windows) a un dominio de prueba `guardduty2activityb.com`.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/DenialOfService.Dns

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) mediante el protocolo DNS.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico DNS saliente. Esto puede indicar que la instancia que aparece en la lista se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo DNS.

 Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/DenialOfService.Tcp

Una instancia EC2 se comporta de una manera que indica que se está utilizando para realizar un ataque de denegación de servicio (DoS) mediante el protocolo TCP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico TCP saliente. Esto puede indicar que la instancia se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo TCP.

 Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/DenialOfService.Udp

Una instancia EC2 se comporta de una manera que indica que se está utilizando para realizar un ataque de denegación de servicio (DoS) mediante el protocolo UDP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico UDP saliente. Esto puede indicar que la instancia que aparece en la lista se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo UDP.

Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) mediante el protocolo UDP en un puerto TCP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico UDP saliente cuyo objetivo es un puerto que usualmente se utiliza para la comunicación mediante TCP. Esto puede indicar que la instancia que aparece en la lista se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo UDP a un puerto TCP.

 Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/DenialOfService.UnusualProtocol

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) utilizando un protocolo inusual.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico saliente mediante un tipo de protocolo inusual que no suelen utilizar las instancias de EC2 (por ejemplo, el protocolo de administración de grupos de Internet). Esto puede indicar que la instancia se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante un protocolo inusual. Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/Spambot

Una instancia de EC2 exhibe un comportamiento inusual al comunicarse con un host remoto en el puerto 25.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS se está comunicando con un host remoto en el puerto 25. Este comportamiento es inusual, ya que esta instancia de EC2 no tiene un historial previo de comunicaciones en el puerto 25. El puerto 25 lo utilizan tradicionalmente los servidores de correo para las comunicaciones SMTP. Este resultado indica que la instancia EC2 es posible que se vea comprometida para su uso en el envío de spam.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Behavior:EC2/NetworkPortUnusual

Una instancia EC2 se comunica con un host remoto en un puerto de servidor inusual.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene historial previo de comunicaciones en este puerto remoto.

Note

Si la instancia de EC2 se ha comunicado en los puertos 389 o 1389, la gravedad del resultado asociado se modificará a Alta y los campos del resultado incluirán el siguiente valor:

- `service.additionalInfo.context = Possible log4j callback`

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Behavior:EC2/TrafficVolumeUnusual

Una instancia EC2 genera una cantidad inusualmente elevada de tráfico de red a un host remoto.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene historial previo de envío de esta cantidad de tráfico a este host remoto.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

CryptoCurrency:EC2/BitcoinTool.B

Una instancia EC2 consulta una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría ser la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:EC2/BitcoinTool.B`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

CryptoCurrency:EC2/BitcoinTool.B!DNS

Una instancia EC2 consulta un nombre de dominio asociado con la actividad relacionada con la criptomoneda.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría ser la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:EC2/BitcoinTool.B!DNS`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

DefenseEvasion:EC2/UnusualDNSResolver

Una instancia de Amazon EC2 se está comunicando con un solucionador de DNS público inusual.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene un historial reciente de comunicación con este solucionador de DNS público. El campo Inusual del panel de detalles de resultado de la consola de GuardDuty puede proporcionar información sobre el solucionador de DNS consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

DefenseEvasion:EC2/UnusualDoHActivity

Una instancia de Amazon EC2 se comunica de manera inusual con un DNS a través de HTTPS (DoH).

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene ningún historial reciente de comunicaciones de DNS a través de HTTPS (DoH) con este servidor DoH público. El campo Inusual de los detalles de resultado puede proporcionar información sobre el servidor de DoH consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

DefenseEvasion:EC2/UnusualDoTActivity

Una instancia de Amazon EC2 se está comunicando de manera inusual con un DNS a través de TLS (DoT).

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene ningún historial reciente de comunicaciones de DNS a través de TLS (DoT) con este servidor DoT público. El campo Inusual del panel de detalles de resultado puede proporcionar información sobre el servidor DoT consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/AbusedDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que está asociado a dominios que se sabe que se han utilizado indebidamente.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que se han utilizado indebidamente. Algunos ejemplos de dominios utilizados indebidamente son los nombres de dominio de nivel superior (TLD) y los nombres de dominio de segundo nivel (2LD), que proporcionan registros de subdominios gratuitos, así como proveedores de DNS dinámicos. Los actores de amenazas suelen utilizar estos servicios para registrar dominios de forma gratuita o a un bajo costo. Los dominios de baja reputación de esta categoría también pueden ser dominios caducados que se resuelven en la dirección IP de estacionamiento de un registrador y, por lo tanto, es posible que ya no estén activos. Una IP de estacionamiento es el lugar al que un registrador dirige el tráfico de dominios que no se han vinculado a ningún servicio. La instancia de Amazon EC2 que aparece en la lista puede haberse visto afectada, ya que los actores de amenazas suelen utilizar estos registradores o servicios para la distribución de C&C y malware.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/BitcoinDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que está asociado a la actividad relacionada con criptomonedas.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría representar la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Impact:EC2/BitcoinDomainRequest.Reputation`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/MaliciousDomainRequest.Reputation

Una instancia de EC2 consulta un dominio de baja reputación que está asociado a dominios maliciosos conocidos.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que son maliciosos. Por ejemplo, los dominios pueden estar asociados a una dirección IP conocida como oculta. Los dominios ocultos son aquellos

que anteriormente estaban controlados por un agente de amenazas y las solicitudes que se les hagan pueden indicar que la instancia se ha visto afectada. Estos dominios también pueden estar correlacionados con campañas o algoritmos de generación de dominios maliciosos conocidos.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/MaliciousDomainRequest.Custom

La instancia de EC2 está consultando un dominio en una lista de entidades de amenazas personalizada.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado informa que la instancia de Amazon EC2 mostrada en el entorno de AWS está consultando un nombre de dominio incluido en la lista de entidades de amenazas personalizada que cargó y activó. En GuardDuty, una lista de entidades de amenazas está formada por direcciones IP y nombres de dominio maliciosos conocidos. GuardDuty genera resultados basados en la actividad asociada a la lista de entidades de amenazas cargada. Puede ver el nombre de esta lista de entidades de amenazas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/PortSweep

Una instancia de EC2 está sondeando un puerto en un gran número de direcciones IP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está sondeando un puerto en un gran número de direcciones IP direccionables públicamente. Este tipo de actividad se suele utilizar para encontrar hosts vulnerables y explotarlos. En el panel de detalles de resultado de la consola de GuardDuty, solo se muestra la dirección IP remota más reciente

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/SuspiciousDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que resulta sospechoso por naturaleza debido a su antigüedad o a su baja popularidad.

Gravedad predeterminada: baja

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación que se sospecha que es malicioso. Se observaron características de este dominio que eran consistentes con las de dominios maliciosos observados anteriormente; sin embargo, nuestro modelo de reputación no pudo relacionarlo definitivamente con una amenaza conocida. Por lo general, estos dominios se han detectado recientemente o reciben poco tráfico.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Impact:EC2/WinRMBruteForce

Una instancia de EC2 está realizando un ataque de fuerza bruta saliente con Windows Remote Management.

Gravedad predeterminada: baja*

Note

La gravedad de este resultado es baja si su instancia de EC2 era el objetivo de un ataque de fuerza bruta. La gravedad de este resultado es alta si su instancia de EC2 es el actor que se utiliza para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que está llevando a cabo un ataque de Windows Remote Management (WinRM) con fuerza bruta con el objetivo de obtener acceso al servicio de Windows Remote Management en sistemas basados en Windows.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Recon:EC2/PortProbeEMRUnprotectedPort

Una instancia de EC2 tiene un puerto relacionado con EMR desprotegido sondeado por un host malicioso conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado informa de que un puerto sensible relacionado con EMR en la instancia de EC2 de la lista que forma parte de un clúster en el entorno de AWS no está bloqueado por un grupo de

seguridad, una lista de control de acceso (ACL) o un firewall en el host, como IPTables de Linux. Además, este resultado informa de que analizadores conocidos en Internet sondean activamente este puerto. Los puertos que pueden desencadenar este resultado, como el puerto 8088 (puerto de IU web de YARN), se pueden utilizar potencialmente para la ejecución de código remoto.

Recomendaciones de corrección:

Debería bloquear el acceso libre a los puertos en los clústeres desde Internet y restringir el acceso solo a direcciones IP específicas que requieren acceso a estos puertos. Para obtener más información, consulte [Grupos de seguridad para clústeres de EMR](#).

Recon:EC2/PortProbeUnprotectedPort

Una instancia EC2 tiene un puerto sin protección que un host malintencionado conocido está sondeando.

Gravedad predeterminada: baja*

Note

La gravedad predeterminada de este resultado es Baja. Sin embargo, si el puerto sondeado es utilizado por Elasticsearch (9200 o 9300), la gravedad del resultado es Alta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que un puerto en la instancia de EC2 que aparece en la lista del entorno de AWS no está bloqueado por un grupo de seguridad, una lista de control de acceso (ACL) o un firewall del host (por ejemplo, IPTables) y está siendo sondeado activamente por análisis conocidos en Internet.

Si el puerto desprotegido identificado es 22 o 3389 y utiliza estos puertos para conectarse a la instancia, aún puede limitar la exposición permitiendo el acceso a estos puertos solo a las direcciones IP desde el espacio de direcciones IP de la red corporativa. Para restringir el acceso al puerto 22 en Linux, consulte [Autorización del tráfico de entrada para sus instancias de Linux](#). Para restringir el acceso al puerto 3389 en Windows, consulte [Autorización del tráfico de entrada para sus instancias de Windows](#).

GuardDuty no genera este resultado para los puertos 443 y 80.

Recomendaciones de corrección:

Puede haber casos en los que las instancias se expongan de forma intencionada, por ejemplo, si están alojando servidores web. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de Recon:EC2/PortProbeUnprotectedPort. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Recon:EC2/Portscan

Una instancia EC2 realiza exploraciones de puertos salientes a un host remoto.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está involucrada en un posible ataque de análisis de puertos porque está intentando conectarse a varios puertos en un período corto de tiempo. El objetivo de un ataque de análisis de puertos es localizar puertos abiertos para detectar los servicios que está ejecutando el equipo e identificar su sistema operativo.

Recomendaciones de corrección:

Este resultado puede ser un falso positivo cuando se implementan aplicaciones de evaluación de vulnerabilidades en instancias de EC2 en su entorno, ya que estas aplicaciones analizan los puertos para alertarle sobre puertos abiertos mal configurados. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de Recon:EC2/Portscan. El segundo criterio de filtro debe coincidir con

la instancia o instancias que alojan estas herramientas de evaluación de vulnerabilidades. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/BlackholeTraffic

Una instancia EC2 intenta comunicarse con una dirección IP de un host remoto que es un agujero negro conocido.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está intentando comunicarse con una dirección IP de agujero negro (u oculta). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/BlackholeTraffic!DNS

Una instancia EC2 consulta un nombre de dominio que se está redireccionando a una dirección IP de agujero negro.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que una instancia de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro. Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/DGADomainRequest.B

Una instancia EC2 consulta dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar una instancia EC2 comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está intentando hacer consultas en dominios de algoritmos de generación de dominios (DGA). Su instancia EC2 podría estar en peligro.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C&C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

Note

Este resultado se basa en el análisis de nombres de dominio mediante heurística avanzada, por lo que podría identificar nuevos dominios de DGA que no están presentes en fuentes de información de amenazas.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/DGADomainRequest.C!DNS

Una instancia EC2 consulta dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar una instancia EC2 comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está intentando hacer consultas en dominios de algoritmos de generación de dominios (DGA). Su instancia EC2 podría estar en peligro.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C&C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

Note

Este resultado se basa en dominios de DGA conocidos de las fuentes de información de amenazas de GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/DNSDataExfiltration

Una instancia EC2 sustrae datos a través de consultas de DNS.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está ejecutando malware que utiliza consultas de DNS para transferencias de datos salientes. Este tipo de transferencia de datos indica que se trata de una instancia afectada y podría provocar la exfiltración de datos. Por lo general, el tráfico de DNS no está bloqueado por los firewalls. Por ejemplo, el malware de una instancia de EC2 comprometida puede codificar datos (como el número de la tarjeta de crédito) en una consulta de DNS y enviarlos a un servidor DNS remoto controlado por un atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/DriveBySourceTraffic!DNS

Una instancia EC2 consulta un nombre de dominio de un host remoto que es una fuente conocida de ataques de descarga Drive-By.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio de un host remoto que es un origen conocido de ataques de descargas Drive-By. Se trata de descargas no deseadas de software informático desde Internet que pueden desencadenar la instalación automática de un virus, spyware o malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/DropPoint

Una instancia EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 de su entorno de AWS está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/DropPoint!DNS

Una instancia EC2 está consultando un nombre de dominio de un host remoto que se conoce que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que una instancia de EC2 de su entorno de AWS está consultando un nombre de dominio de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Trojan:EC2/PhishingDomainRequest!DNS

Una instancia EC2 consulta dominios implicados en ataques de phishing. Su instancia EC2 podría estar en peligro.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que está intentando hacer consultas a un dominio implicado en ataques de suplantación de identidad. Los dominios de suplantación de identidad los configura alguien que se presenta como una institución legítima para inducir a las personas a proporcionar información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas. Es posible que su instancia de EC2 esté intentando recuperar datos confidenciales almacenados en un sitio web de suplantación de identidad o que esté intentando configurar un sitio web de este tipo. Su instancia EC2 podría estar en peligro.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Una instancia de EC2 establece conexiones con una dirección IP en una lista de amenazas personalizada.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS se está comunicando con una dirección IP incluida en una lista de amenazas que ha cargado. En GuardDuty, una lista de amenazas está formada por direcciones IP maliciosas conocidas. GuardDuty genera resultados basados en las listas de amenazas cargadas. La lista de amenazas utilizada para generar este resultado se mostrará en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

UnauthorizedAccess:EC2/MetadataDNSRebind

Una instancia de EC2 está haciendo búsquedas de DNS que se resuelven en el servicio de metadatos de la instancia.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que una instancia de EC2 del entorno de AWS está consultando un dominio que se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Una consulta de DNS de este tipo puede indicar que la instancia es el objetivo de una técnica de reenlace de DNS. Esta técnica se puede utilizar para obtener metadatos de una instancia de EC2, que incluye las credenciales de IAM asociadas a la instancia.

El reenlace de DNS implica engañar a una aplicación que se ejecuta en la instancia de EC2 para que cargue datos devueltos desde una URL, de tal forma que el nombre de dominio de la URL se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Esto hace que la aplicación obtenga acceso a los metadatos de EC2 y, posiblemente, los ponga a disposición del atacante.

Solo se puede obtener acceso a los metadatos de EC2 mediante el reenlace de DNS si la instancia de EC2 ejecuta una aplicación vulnerable que permite la inserción de URL o si un usuario obtiene acceso a la URL en un navegador web que se ejecuta en la instancia de EC2.

Recomendaciones de corrección:

En respuesta a este resultado, es importante evaluar si hay alguna aplicación vulnerable que se esté ejecutando en la instancia de EC2 o si un usuario ha utilizado un navegador para acceder al dominio identificado en el resultado. Si la causa raíz es una aplicación vulnerable, debe corregir la vulnerabilidad. Si un usuario ha navegado por el dominio identificado, debe bloquear el dominio o impedir que los usuarios puedan acceder a él. Si determina que el resultado está relacionado con cualquiera de los casos anteriores, debe [revocar la sesión asociada a la instancia de EC2](#).

Algunos clientes de AWS asignan deliberadamente la dirección IP de metadatos a un nombre de dominio en sus servidores DNS autorizados. Si este es el caso en su entorno de , le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de UnauthorizedAccess:EC2/MetaDataDNSRebind. El segundo criterio de filtro debe ser Dominio de la solicitud DNS y el valor debe coincidir con el dominio que ha mapeado a la dirección IP de metadatos (169.254.169.254). Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

UnauthorizedAccess:EC2/RDPBruteForce

Una instancia EC2 se ve implicada en ataques de fuerza bruta RDP.

Gravedad predeterminada: baja*

Note

La gravedad de este resultado es baja si su instancia de EC2 era el objetivo de un ataque de fuerza bruta. La gravedad de este resultado es alta si su instancia de EC2 es el actor que se utiliza para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS se ha visto envuelta en un ataque de fuerza bruta cuyo objetivo ha sido obtener contraseñas de servicios de RDP en sistemas basados en Windows. Esto puede significar un acceso no autorizado a los recursos de AWS.

Recomendaciones de corrección:

Si el Rol de recurso de su instancia es ACTOR, indica que su instancia se ha utilizado para llevar a cabo ataques de fuerza bruta a RDP. A no ser que esta instancia tenga un motivo legítimo para contactar con la dirección IP mostrada en la lista como Target, se recomienda que asuma que su instancia se ha visto afectada y lleve a cabo las acciones que aparecen en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Si el Rol de recurso de su instancia es TARGET, este resultado puede corregirse mediante la delegación de la protección de su puerto RDP solo a direcciones IP de confianza a través de grupos de seguridad, ACL o firewalls. Para obtener más información, consulte [Tips for securing your EC2 instances \(Linux\)](#).

UnauthorizedAccess:EC2/SSHBruteForce

Una instancia EC2 se ve implicada en ataques de fuerza bruta SSH.

Gravedad predeterminada: baja*

Note

La gravedad de este resultado es baja si se dirige un ataque de fuerza a una de las instancias de EC2. La gravedad de este resultado es alta si la instancia de EC2 se está utilizando para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS se ha visto envuelta en un ataque de fuerza bruta cuyo objetivo ha sido obtener contraseñas de servicios de SSH en sistemas basados en Linux. Esto puede significar un acceso no autorizado a los recursos de AWS.

Note

Este resultado solo se genera mediante el monitoreo del tráfico en el puerto 22 por parte de . Si los servicios de SSH están configurados para usar otros puertos, no se genera este resultado.

Recomendaciones de corrección:

Si el objetivo del intento de fuerza bruta es un host bastión, esto podría representar el comportamiento esperado para su entorno de AWS. Si este es el caso, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/SSHBruteForce`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de la instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad no se espera en su entorno y el Rol de recurso de su instancia es `TARGET`, este resultado puede corregirse mediante la delegación de la protección de su puerto SSH solo a direcciones IP de confianza a través de grupos de seguridad, ACL o firewalls. Para obtener más información, consulte [Tips for securing your EC2 instances \(Linux\)](#).

Si el Rol de recurso de su instancia es `ACTOR`, indica que la instancia se ha utilizado para llevar a cabo ataques de fuerza bruta a SSH. A no ser que esta instancia tenga un motivo legítimo para contactar con la dirección IP mostrada en la lista como `Target`, se recomienda que asuma que su instancia se ha visto afectada y lleve a cabo las acciones que aparecen en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

UnauthorizedAccess:EC2/TorClient

La instancia EC2 está estableciendo conexiones con un guardia Tor o un nodo Authority.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS está estableciendo conexiones con un nodo Authority o Guard de Tor. Tor es un software que permite la comunicación anónima. Los nodos Guard y Authority de Tor actúan como puertas de enlace a una red de Tor. Este tráfico puede indicar que esta instancia de EC2 se ha visto afectada y está actuando como cliente en

una red de Tor. Este resultado puede significar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

UnauthorizedAccess:EC2/TorRelay

La instancia EC2 establece conexiones a una red Tor como repetidor Tor.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS está estableciendo conexiones con una red de Tor de una forma que sugiere que actúa como un relé de Tor. Tor es un software que permite la comunicación anónima. Tor incrementa el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Tipos de resultados de IAM con GuardDuty

Los siguientes resultados son específicos de las entidades y claves de acceso de IAM y siempre tendrán un Tipo de recurso de AccessKey. La gravedad y los detalles de los resultados varían en función del tipo de resultado.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para obtener más información, consulte [Orígenes de datos fundamentales de GuardDuty](#).

En el caso de todos los resultados relacionados con IAM, se recomienda que examine la entidad en cuestión y se asegure de que sus permisos sigan las prácticas recomendadas de privilegio mínimo. Si la actividad es inesperada, las credenciales pueden verse afectadas. Para obtener más información sobre los resultados de corrección, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Temas

- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [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/TorIPCaller](#)

CredentialAccess:IAMUser/AnomalousBehavior

Se ha invocado una API utilizada para acceder a un entorno de AWS de forma anómala.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a la fase de acceso a las credenciales en un ataque, donde un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su entorno. Las API de esta categoría son GetPasswordData, GetSecretValue, BatchGetSecretValue y GenerateDbAuthToken.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

DefenseEvasion:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API utilizada para evadir las medidas defensivas.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus rastros para evitar ser detectado. Las API de esta categoría suelen eliminar, deshabilitar o detener operaciones, como `DeleteFlowLogs`, `DisableAlarmActions` o `StopLogging`.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Discovery:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para detectar recursos.

Gravedad predeterminada: baja

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada se suele asociar a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de sufrir un ataque más amplio. Las API de esta categoría suelen obtener, describir o enumerar operaciones, como `DescribeInstances`, `GetRolePolicy` o `ListAccessKeys`.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta

e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Exfiltration:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para recopilar datos de un entorno de AWS.

Gravedad predeterminada: alta

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de exfiltración, en las que un adversario intenta recopilar datos de su red mediante el empaquetado y el cifrado para evitar ser detectado. Las API para este tipo de resultado son únicamente operaciones de administración (plano de control) y, por lo general, están relacionadas con S3, instantáneas y bases de datos, como PutBucketReplication, CreateSnapshot o RestoreDBInstanceFromDBSnapshot.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Impact:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para manipular datos o procesos de un entorno de AWS.

Gravedad predeterminada: alta

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta interrumpir las operaciones y manipular, interrumpir o destruir los datos de la cuenta. Las API para este tipo de resultado suelen eliminar, actualizar o preparar operaciones, como DeleteSecurityGroup, UpdateUser o PutBucketPolicy.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

InitialAccess:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que suele utilizarse para obtener acceso no autorizado a un entorno de AWS.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a la fase de acceso inicial de un ataque, cuando un adversario intenta establecer acceso a su entorno. Las API de esta categoría suelen obtener operaciones de token o de sesión, como `StartSession` o `GetAuthorizationToken`.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PenTest:IAMUser/KaliLinux

Se invocó una API desde una máquina Kali Linux.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que una máquina que ejecuta Kali Linux está haciendo llamadas a la API mediante credenciales que pertenecen a la cuenta de AWS que aparece en la lista de su entorno. Kali Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PenTest:IAMUser/ParrotLinux

Se ha invocado una API desde una máquina Parrot Security Linux.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que una máquina que ejecuta Parrot Security Linux está haciendo llamadas a la API mediante unas credenciales que pertenecen a la cuenta de AWS que aparece en la lista de su entorno. Parrot Security Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PenTest:IAMUser/PentooLinux

Se ha invocado una API desde una máquina Pentoo Linux.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que una máquina que ejecuta Pentoo Linux está haciendo llamadas a la API mediante credenciales que pertenecen a la cuenta de AWS que aparece en la lista de su entorno. Pentoo Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Persistence:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que suele utilizarse para conservar acceso no autorizado a un entorno de AWS.

Gravedad predeterminada: media

- Origen de datos: evento de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder a su entorno e intenta conservar ese acceso. Las API de esta categoría suelen crear, importar o modificar operaciones, como `CreateAccessKey`, `ImportKeyPair` o `ModifyInstanceAttribute`.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Policy:IAMUser/RootCredentialUsage

Se ha invocado una API mediante credenciales de inicio de sesión del usuario raíz.

Gravedad predeterminada: baja

- Origen de datos: eventos de administración de CloudTrail o eventos de datos de CloudTrail para S3

Este resultado le informa de que las credenciales de inicio de sesión del usuario raíz de la Cuenta de AWS que aparece en la lista de su entorno se están utilizando para hacer solicitudes a los servicios de AWS. Se recomienda que los usuarios nunca utilicen las credenciales de inicio de sesión del usuario raíz para acceder a los servicios de AWS. En su lugar, se debe acceder a los servicios de AWS con credenciales temporales con privilegios mínimos de AWS Security Token Service (STS). En los casos donde no se admite AWS STS, se recomienda utilizar las credenciales de usuario de IAM. Para obtener más información, consulte las [prácticas recomendadas de IAM](#).

 Note

Si la protección para S3 está habilitada para la cuenta, este resultado se puede generar en respuesta a los intentos de ejecutar operaciones de plano de datos de S3 en recursos de Amazon S3 con credenciales de inicio de sesión de usuario raíz de la Cuenta de AWS. La llamada a la API utilizada se mostrará en los detalles de resultado. Si la S3 Protection no está habilitada, este resultado solo se puede activar mediante las API de registro de eventos. Para obtener más información sobre la protección para S3, consulte [Protección de S3](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Policy: IAMUser/ShortTermRootCredentialUsage

Se ha invocado una API mediante el uso de credenciales de usuario raíz restringidas.

Gravedad predeterminada: baja

- Origen de datos: eventos de administración de AWS CloudTrail o eventos de datos de AWS CloudTrail de S3

Este resultado le informa que las credenciales de usuario creadas para la Cuenta de AWS que aparece en la lista de su entorno se están utilizando para hacer solicitudes a los Servicios de AWS.

Se recomienda que utilice sus credenciales de usuario raíz únicamente para realizar [tareas que requieran credenciales de usuario raíz](#).

Cuando sea posible, acceda a los Servicios de AWS mediante roles de IAM con privilegios mínimos con credenciales temporales de AWS Security Token Service (AWS STS). En los casos en los que AWS STS no se admite, la mejor práctica es utilizar las credenciales de usuario de IAM. Para más información, consulte [Prácticas recomendadas de seguridad en IAM](#) y las [Prácticas recomendadas de usuario raíz para su Cuenta de AWS](#) en la Guía de usuario de IAM.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PrivilegeEscalation:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para obtener permisos de nivel superior a un entorno de AWS.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de derivación de privilegios, en las que un adversario intenta obtener permisos de nivel superior para acceder a un entorno. Las API de esta categoría suelen implicar operaciones que cambian las políticas, los roles y los usuarios de IAM, como `AssociateIamInstanceProfile`, `AddUserToGroup` o `PutUserPolicy`.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Recon:IAMUser/MaliciousIPCaller

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS se ha invocado desde una dirección IP que aparece en una lista de amenazas. Un atacante puede utilizar credenciales robadas para llevar a cabo este tipo de reconocimiento de sus recursos de AWS y encontrar de esta manera más credenciales valiosas o determinar cuáles son las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Recon:IAMUser/MaliciousIPCaller.Custom

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS en una cuenta dentro de su entorno se ha invocado desde una dirección IP que aparece en una lista de amenazas personalizada. La lista de amenazas utilizada se mostrará en los detalles del resultado. Un atacante podría utilizar credenciales robadas para llevar a cabo este tipo de reconocimiento de sus recursos de AWS y encontrar de esta manera más credenciales valiosas o determinar cuáles son las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Recon:IAMUser/TorIPCaller

Se ha invocado una API desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS de una cuenta dentro de su entorno se ha invocado desde una dirección IP de nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Un atacante utilizaría Tor para ocultar su verdadera identidad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Stealth:IAMUser/CloudTrailLoggingDisabled

Los registros de AWS CloudTrail se han desactivado.

Gravedad predeterminada: baja

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que se ha desactivado un registro de seguimiento de CloudTrail dentro de su entorno de AWS. Puede tratarse del intento por parte de un atacante de desactivar el registro para cubrir sus rastros mediante la eliminación de cualquier indicio de su actividad y, a su vez, la obtención de acceso a los recursos de AWS con fines maliciosos. Este resultado se puede desencadenar mediante una eliminación o actualización correcta de un registro de seguimiento. Este resultado también se puede desencadenar mediante una eliminación exitosa de un bucket de S3 que almacena los registros de un seguimiento asociado con GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Stealth:IAMUser/PasswordPolicyChange

La política de contraseñas de la cuenta se ha debilitado.

Gravedad predeterminada: baja*

Note

La gravedad de este resultado puede ser baja, media o alta, según la gravedad de los cambios hechos en la política de contraseñas.

- Origen de datos: eventos de administración de CloudTrail

La política de contraseñas de las cuentas de AWS estaba debilitada en la cuenta que aparece en la lista dentro de su entorno de AWS. Por ejemplo, se ha eliminado o actualizado para exigir menos caracteres, no requerir símbolos y números, o se ha requerido la ampliación del periodo de vencimiento de la contraseña. Este resultado también se puede desencadenar mediante un intento de actualización o de eliminación de la política de contraseñas de la cuenta de AWS. La política de contraseñas de la cuenta de AWS define las reglas que determinan los tipos de contraseñas que se pueden establecer para los usuarios de IAM. Una política de contraseñas más débil permite la creación de contraseñas que son fáciles de recordar y potencialmente más fáciles de adivinar, y que suponen un riesgo para la seguridad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Se han observado varios inicios de sesión correctos en la consola desde distintos lugares del mundo.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que se han observado varios inicios de sesión correctos en la consola para el mismo usuario de IAM aproximadamente al mismo tiempo en diversas ubicaciones geográficas. Estos patrones de ubicación de acceso anómalo y arriesgado indican un posible acceso no autorizado a los recursos de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Se están utilizando las credenciales creadas exclusivamente para una instancia de EC2 a través de un rol de lanzamiento de instancias desde otra cuenta dentro de AWS.

Gravedad predeterminada: alta*

Note

La gravedad predeterminada de este resultado es alta. Sin embargo, si una cuenta afiliada a su entorno de AWS ha invocado la API, la gravedad es media.

- Origen de datos: eventos de administración de CloudTrail o eventos de datos de CloudTrail para S3

Este resultado informa de cuándo se utilizan las credenciales de la instancia de Amazon EC2 para invocar API desde una dirección IP o un punto de conexión de Amazon VPC que pertenece a una cuenta de AWS diferente de aquella en la que se ejecuta la instancia de Amazon EC2 asociada. La detección de puntos de conexión de VPC solo está disponible para los servicios que admiten eventos de actividad de red para puntos de conexión de VPC. Para obtener información sobre los servicios

que admiten eventos de actividad de red para puntos de conexión de VPC, consulte [Registro de eventos de actividad de red](#) en la Guía del usuario de AWS CloudTrail.

AWS no recomienda redistribuir credenciales temporales fuera de la entidad que las ha creado (por ejemplo, las aplicaciones de AWS Lambda, Amazon EC2 o AWS). Sin embargo, los usuarios autorizados pueden exportar credenciales desde las instancias de Amazon EC2 para realizar llamadas a la API legítimas. Si el campo `remoteAccountDetails.Affiliated` es `True`, se ha invocado la API desde una cuenta asociada a la misma cuenta de administrador. Para descartar un posible ataque y verificar la legitimidad de la actividad, póngase en contacto con el propietario de la Cuenta de AWS o la entidad principal de IAM a la que se han asignado estas credenciales.

 Note

Si GuardDuty observa una actividad continua desde una cuenta remota, su modelo de machine learning (ML) lo identificará como un comportamiento esperado. Por lo tanto, GuardDuty dejará de generar este resultado para la actividad de esa cuenta remota. GuardDuty seguirá generando resultados sobre el nuevo comportamiento de otras cuentas remotas y volverá a evaluar las cuentas remotas aprendidas a medida que el comportamiento cambie.

Recomendaciones de corrección:

Este resultado se genera cuando se realizan solicitudes a la API de AWS dentro de AWS a través de una instancia de Amazon EC2 fuera de la Cuenta de AWS, mediante el uso de las credenciales de sesión de la instancia de Amazon EC2. Puede ser habitual, como en el caso de la arquitectura de puerta de enlace de tránsito en una configuración de [centro y radios](#), dirigir el tráfico a través de una única VPC de egreso central con puntos de conexión de servicios de AWS. Si este es el comportamiento previsto, GuardDuty recomienda utilizar [Reglas de supresión](#) y crear una regla con un criterio de dos filtros. El primer criterio es el tipo de resultado, que en este caso es `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS`. El segundo criterio de filtrado es el ID de cuenta remota de los detalles de la cuenta remota.

En respuesta a este resultado, puede utilizar el siguiente flujo de trabajo para determinar el curso de acción:

1. Identifique la cuenta remota implicada en el campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.

2. Determine si esa cuenta está afiliada al entorno de GuardDuty desde el campo `service.action.awsApiCallAction.remoteAccountDetails.affiliated`.
3. Si la cuenta está afiliada, contacte al propietario de la cuenta remota y al propietario de las credenciales de la instancia de Amazon EC2 para investigar.

Si la cuenta no está afiliada, el primer paso es evaluar si esa cuenta está asociada a la organización pero no forma parte del entorno de múltiples cuentas de GuardDuty configurado, o si GuardDuty aún no ha sido habilitado en esta cuenta. A continuación, contacte al propietario de las credenciales de la instancia de Amazon EC2 para determinar si existe un caso de uso que amerite que una cuenta remota utilice estas credenciales.

4. Si el propietario de las credenciales no reconoce la cuenta remota, es posible que un actor de amenazas que opere dentro de AWS haya puesto en peligro las credenciales. Debe seguir los pasos que se recomiendan en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#) para proteger el entorno.

Además, puede [enviar un informe de uso indebido](#) al equipo de Seguridad y confianza de AWS para iniciar una investigación sobre la cuenta remota. Al enviar el informe al equipo de Seguridad y confianza de AWS, incluya todos los detalles del resultado en JSON.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Las credenciales creadas exclusivamente para una instancia EC2 a través de un rol de lanzamiento de instancias se utilizan desde una dirección IP externa.

Gravedad predeterminada: alta

- Origen de datos: eventos de administración de CloudTrail o eventos de datos de CloudTrail para S3

Este resultado le informa de que un host fuera de AWS ha intentado ejecutar operaciones de API de AWS mediante credenciales de AWS temporales que se crearon en una instancia de EC2 dentro de su entorno de AWS. La instancia de EC2 que aparece en la lista podría haberse visto afectada y las credenciales temporales de esta instancia podrían haberse exfiltrado a un host remoto fuera de AWS. AWS no recomienda redistribuir las credenciales temporales fuera de la entidad que las creó (por ejemplo, aplicaciones de AWS, EC2 o Lambda). Sin embargo, los usuarios autorizados pueden exportar credenciales desde sus instancias de EC2 para realizar llamadas a la API legítimas. Para

descartar un posible ataque y verificar la legitimidad de la actividad, valide si se espera el uso de credenciales de instancia por parte de la IP remota en el resultado.

 Note

Si GuardDuty observa una actividad continua desde una cuenta remota, su modelo de machine learning (ML) lo identificará como un comportamiento esperado. Por lo tanto, GuardDuty dejará de generar este resultado para la actividad de esa cuenta remota. GuardDuty seguirá generando resultados sobre el nuevo comportamiento de otras cuentas remotas y volverá a evaluar las cuentas remotas aprendidas a medida que el comportamiento cambie.

Recomendaciones de corrección:

Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de [AWS Outposts](#) o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si se trata de un comportamiento esperado, se recomienda utilizar reglas de supresión y crear una regla que conste de dos criterios de filtrado. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. El segundo criterio de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR de su puerta de enlace de Internet en las instalaciones. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

 Note

Si GuardDuty observa una actividad continua de un origen externa, su modelo de machine learning identificará este comportamiento como esperado y dejará de generar este resultado para la actividad de ese origen. GuardDuty seguirá generando resultados sobre el nuevo comportamiento de otros orígenes y volverá a evaluar los orígenes aprendidos a medida que el comportamiento cambie.

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que una operación de la API (por ejemplo, un intento de lanzar una instancia de EC2, crear un nuevo usuario de IAM o modificar los privilegios de AWS) se ha invocado desde una dirección IP maliciosa conocida. Esto puede significar un acceso no autorizado a los recursos de AWS dentro de su entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Se ha invocado una API desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que una operación de la API (por ejemplo, un intento de lanzar una instancia de EC2, crear un nuevo usuario de IAM o modificar los privilegios de AWS) se ha invocado desde una dirección IP incluida en una lista de amenazas que se ha cargado. En GuardDuty, una lista de amenazas está formada por direcciones IP maliciosas conocidas. Esto puede significar un acceso no autorizado a los recursos de AWS dentro de su entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:IAMUser/TorIPCaller

Se ha invocado una API desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: media

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que una operación de la API (por ejemplo, un intento de lanzar una instancia de EC2, crear un nuevo usuario de IAM o modificar los privilegios de AWS) se ha invocado desde una dirección IP de nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Tipos de resultados de secuencias de ataque de GuardDuty

GuardDuty detecta una secuencia de ataque cuando una secuencia específica de múltiples acciones se alinea con una actividad potencialmente sospechosa. Una secuencia de ataque incluye señales como las actividades de la API y los resultados de GuardDuty. Cuando GuardDuty observa un grupo de señales en una secuencia específica que indican una amenaza de seguridad en avance, en curso o reciente, GuardDuty genera un resultado de la secuencia de ataque. GuardDuty considera que las actividades individuales de la API no se presentan como [weak signals](#) porque no se presentan como una amenaza potencial.

Las detecciones de secuencias de ataques se centran en la posibilidad de comprometer los datos de Amazon S3 (que pueden formar parte de un ataque de ransomware más amplio), las credenciales de AWS comprometidas y los clústeres de Amazon EKS comprometidos. En las siguientes secciones, se proporciona información sobre cada una de las secuencias de ataque.

Temas

- [AttackSequence:EKS/CompromisedCluster](#)

- [AttackSequence:IAM/CompromisedCredentials](#)
- [AttackSequence:S3/CompromisedData](#)

AttackSequence:EKS/CompromisedCluster

Secuencia de acciones sospechosas realizadas por un clúster Amazon EKS potencialmente comprometido.

- Gravedad predeterminada: crítica
- Orígenes de datos:
 - [Eventos de registro de auditoría de EKS](#)
 - [Runtime Monitoring de Amazon EKS](#)
 - [Detección de malware de Amazon EKS para Amazon EC2](#)
 - [Eventos de datos de AWS CloudTrail para S3](#)
 - [Eventos de administración de AWS CloudTrail](#)
 - [Logs de flujo de VPC](#)
 - [Registros de consultas de DNS de Route53 Resolver](#)

Este resultado le informa que GuardDuty detectó una secuencia de acciones sospechosas que indican un clúster de Amazon EKS potencialmente comprometido en su entorno. Se observaron varios comportamientos de ataque sospechosos y anómalos, como procesos maliciosos o conexiones con puntos de conexión maliciosos, en el mismo clúster de Amazon EKS.

GuardDuty utiliza sus algoritmos de correlación patentados para observar e identificar la secuencia de acciones realizadas mediante la credencial de IAM. GuardDuty evalúa los resultados de los planes de protección y otras fuentes de señales para identificar patrones de ataque comunes y emergentes. GuardDuty utiliza varios factores para detectar amenazas, como la reputación de la IP, las secuencias de API, la configuración del usuario y los recursos potencialmente afectados.

Medidas correctivas: si este comportamiento es inesperado en su entorno, es posible que su clúster de Amazon EKS esté en peligro. Para obtener una guía completa de correcciones, consulte [Corregir los resultados de EKS Protection](#) y [Corregir los resultados de la Supervisión en tiempo de ejecución](#)

Además, dado que es posible que las credenciales de AWS se hayan visto comprometidas a través del clúster de EKS, consulte [Corregir credenciales de AWS potencialmente comprometidas](#). Para

ver los pasos a seguir para corregir otros recursos que podrían haberse visto afectados, consulte [Corregir los resultados de seguridad detectados en GuardDuty](#).

AttackSequence:IAM/CompromisedCredentials

Secuencia de solicitudes de API que se invocaron con credenciales de AWS potencialmente comprometidas.

- Gravedad predeterminada: crítica
- Origen de datos: [Eventos de administración de AWS CloudTrail](#)

Este resultado le informa de que GuardDuty detectó una secuencia de acciones sospechosas realizadas con credenciales de AWS que afectan a uno o más recursos de su entorno. Se observaron varios comportamientos de ataque sospechosos y anómalos con las mismas credenciales, lo que aumentó la confianza en que se estaba haciendo un uso indebido de las credenciales.

GuardDuty utiliza sus algoritmos de correlación patentados para observar e identificar la secuencia de acciones realizadas mediante la credencial de IAM. GuardDuty evalúa los resultados de los planes de protección y otras fuentes de señales para identificar patrones de ataque comunes y emergentes. GuardDuty utiliza varios factores para detectar amenazas, como la reputación de la IP, las secuencias de API, la configuración del usuario y los recursos potencialmente afectados.

Medidas correctivas: si este comportamiento es inesperado en su entorno, es posible que sus credenciales de AWS se hayan visto comprometidas. Para obtener información sobre los pasos necesarios para solucionarlo, consulte [Corregir credenciales de AWS potencialmente comprometidas](#). Es posible que las credenciales comprometidas se hayan utilizado para crear o modificar recursos adicionales en su entorno, como buckets de Amazon S3, funciones de AWS Lambda o instancias Amazon EC2. Para ver los pasos a seguir para corregir otros recursos que podrían haberse visto afectados, consulte [Corregir los resultados de seguridad detectados en GuardDuty](#).

AttackSequence:S3/CompromisedData

Se invocó una secuencia de solicitudes de API en un posible intento de filtrar o destruir datos en Amazon S3.

- Gravedad predeterminada: crítica

- Orígenes de datos: [Eventos de datos de AWS CloudTrail para S3](#) y [Eventos de administración de AWS CloudTrail](#)

Este resultado le informa que GuardDuty detectó una secuencia de acciones sospechosas indicativas de que los datos estaban en peligro en uno o más buckets de Amazon Simple Storage Service (Amazon S3), mediante el uso de credenciales de AWS potencialmente comprometidas. Se observaron varios comportamientos de ataque sospechosos y anómalos (solicitudes de API), lo que aumentó la confianza en el uso indebido de las credenciales.

GuardDuty utiliza sus algoritmos de correlación para observar e identificar la secuencia de acciones realizadas mediante la credencial de IAM. Luego, GuardDuty evalúa los resultados en los planes de protección y otras fuentes de señales para identificar patrones de ataque comunes y emergentes. GuardDuty utiliza varios factores para detectar amenazas, como la reputación de la IP, las secuencias de API, la configuración del usuario y los recursos potencialmente afectados.

Medidas correctivas: si esta actividad es inesperada en su entorno, es posible que sus credenciales de AWS o los datos de Amazon S3 se hayan filtrado o destruido. Para ver los pasos a seguir para solucionarlo, consulte [Corregir credenciales de AWS potencialmente comprometidas](#) y [Corregir un bucket de S3 potencialmente comprometido](#).

Tipos de resultados de S3 Protection de GuardDuty

Los siguientes resultados son específicos de los recursos de Amazon S3 y tendrán un Tipo de recurso S3Bucket si el origen de datos son Eventos de datos de CloudTrail para S3 o AccessKey si el origen de datos son Eventos de administración de CloudTrail. La gravedad y los detalles de los resultados variarán en función del tipo de resultado y el permiso asociado con el bucket.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para obtener más información sobre orígenes de datos y modelos, consulte [Orígenes de datos fundamentales de GuardDuty](#).

Important

Los resultados con un origen de datos de eventos de datos de CloudTrail para S3 se generan únicamente si la S3 Protection está habilitada. De forma predeterminada, a partir del 31 de julio de 2020, la S3 Protection se habilita cuando una cuenta habilita GuardDuty por primera vez o cuando una cuenta de administrador delegado de GuardDuty habilita GuardDuty en una cuenta de miembro existente. No obstante, cuando un nuevo miembro se

une a la organización de GuardDuty, se aplican las preferencias de habilitación automática definidas por la organización. Para obtener información acerca de las preferencias de habilitación automática, consulte [Configuración de las preferencias de habilitación automática de la organización](#). Para obtener información acerca de cómo habilitar o desactivar la S3 Protection, consulte [Protección de S3 en GuardDuty](#)

Para cualquier resultado del tipo S3Bucket, se recomienda examinar los permisos del bucket en cuestión y los permisos de los usuarios implicados en el resultado. Si la actividad es inesperada, consulte las recomendaciones de corrección que se detallan en [Corregir un bucket de S3 potencialmente comprometido](#).

Temas

- [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

Se ha invocado de forma anómala una API que se utiliza habitualmente para descubrir objetos de S3.

Gravedad predeterminada: baja

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que una entidad de IAM ha invocado una API de S3 para detectar los buckets de S3 en su entorno, como, por ejemplo, `ListObjects`. Este tipo de actividad está asociada a la fase de descubrimiento de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Discovery:S3/MaliciousIPCaller

Se ha invocado una API de S3 que se suele utilizar para detectar recursos en un entorno de AWS desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a la fase de descubrimiento de un ataque, cuando un adversario recopila información sobre su entorno de AWS. Entre los ejemplos se incluyen `GetObjectAcl` y `ListObjects`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Discovery:S3/MaliciousIPCaller.Custom

Se ha invocado una API de S3 desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una API de S3, como `GetObjectAcl` o `ListObjects`, desde una dirección IP que aparece en una lista de amenazas que ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. Este tipo de actividad está asociada a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Discovery:S3/TorIPCaller

Se ha invocado una API de S3 desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una API de S3, como `GetObjectAc1` o `ListObjects`, desde una dirección IP de nodo de salida de Tor. Este tipo de actividad está asociada a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Exfiltration:S3/AnomalousBehavior

Una entidad de IAM ha invocado una API de S3 de forma sospechosa.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado indica que una entidad de IAM está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a la fase de exfiltración de un ataque, en la que un atacante intenta recopilar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde

la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Exfiltration:S3/MaliciousIPCaller

Se ha invocado una API de S3 que se suele utilizar para recopilar datos de un entorno de AWS desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de exfiltración, en las que un adversario intenta recopilar datos de su red. Entre los ejemplos se incluyen GetObject y CopyObject.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Impact:S3/AnomalousBehavior.Delete

Una entidad de IAM ha invocado una API de S3 que intenta eliminar datos de forma sospechosa.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado indica que una entidad de IAM en su entorno de AWS está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a un ataque que intenta eliminar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para determinar si se puede o se debe restaurar la versión anterior del objeto.

Impact:S3/AnomalousBehavior.Permission

Se ha invocado de forma anómala una API que se utiliza habitualmente para establecer los permisos de la lista de control de acceso (ACL).

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa que una entidad de IAM de su entorno de AWS ha actualizado una política de bucket o una ACL en los buckets de S3 de la lista. Este cambio puede exponer públicamente sus buckets de S3 a todos los usuarios de AWS autenticados.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para asegurarse de que no se haya permitido el acceso público a ningún objeto de forma inesperada.

Impact:S3/AnomalousBehavior.Write

Una entidad de IAM ha invocado una API de S3 que intenta escribir datos de forma sospechosa.

Gravedad predeterminada: media

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado indica que una entidad de IAM en su entorno de AWS está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a un ataque que intenta escribir datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad

de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para asegurarse de que esta llamada a la API no haya escrito datos maliciosos o no autorizados.

Impact:S3/MaliciousIPCaller

Se ha invocado una API de S3 que se utiliza habitualmente para manipular datos o procesos de un entorno de AWS desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir datos de su entorno de AWS. Entre los ejemplos se incluyen PutObject y PutObjectAcl.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

PenTest:S3/KaliLinux

Se ha invocado una API de S3 desde una máquina de Kali Linux.

Gravedad predeterminada: media

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que una máquina que ejecuta Kali Linux está haciendo llamadas a la API de S3 con credenciales que pertenecen a su cuenta de AWS. Las credenciales podrían estar comprometidas. Kali Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

PenTest:S3/ParrotLinux

Se ha invocado una API de S3 desde una máquina de Parrot Security Linux.

Gravedad predeterminada: media

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que una máquina que ejecuta Parrot Security Linux está haciendo llamadas a la API de S3 con credenciales que pertenecen a su cuenta de AWS. Las credenciales podrían estar comprometidas. Parrot Security Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

PenTest:S3/PentooLinux

Se ha invocado una API de S3 desde una máquina de Pentoo Linux.

Gravedad predeterminada: media

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que una máquina que ejecuta Pentoo Linux está haciendo llamadas a la API de S3 con credenciales que pertenecen a su cuenta de AWS. Las credenciales podrían estar comprometidas. Pentoo Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Policy:S3/AccountBlockPublicAccessDisabled

Una entidad de IAM ha invocado una API utilizada para desactivar el bloqueo de acceso público de S3 en una cuenta.

Gravedad predeterminada: baja

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que el bloqueo de acceso público de Amazon S3 estaba desactivado en la cuenta. Cuando se activa la configuración de Bloqueo de acceso público de S3, se utiliza para filtrar las políticas o las listas de control de acceso (ACL) en los buckets como medida de seguridad para prevenir la exposición pública involuntaria de datos.

Normalmente, el Bloqueo de acceso público de S3 está desactivado en una cuenta para permitir el acceso público a un bucket o a los objetos que este contiene. Cuando Bloqueo de acceso público de S3 está desactivado para una cuenta, el acceso a sus buckets se controla mediante las políticas, las ACL o la configuración de Bloqueo de acceso público por bucket que se aplique a sus buckets individuales. Esto no necesariamente significa que los buckets se compartan públicamente, pero sí es importante auditar los permisos que se aplican a los buckets para confirmar que proporcionan el nivel de acceso adecuado.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Policy:S3/BucketAnonymousAccessGranted

Una entidad principal de IAM ha concedido acceso a Internet a un bucket de S3 al cambiar las políticas o las ACL del bucket.

Gravedad predeterminada: alta

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que el bucket de S3 que aparece en la lista se ha hecho públicamente accesible en Internet porque una entidad de IAM ha cambiado una política de bucket o una ACL de ese bucket.

Después de detectar un cambio de política o ACL, GuardDuty utiliza el razonamiento automatizado impulsado por [Zelkova](#) para determinar si el bucket es accesible públicamente.

Note

Si las ACL o las políticas de un bucket están configuradas para denegar explícitamente o denegar todo, es posible que este resultado no refleje el estado actual del bucket. Este resultado no reflejará ninguna configuración de [Bloqueo de acceso público de S3](#) que pudiera haberse habilitado para su bucket de S3. En esos casos, el valor `effectivePermission` del resultado se marcará como UNKNOWN.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Policy:S3/BucketBlockPublicAccessDisabled

Una entidad de IAM ha invocado una API utilizada para desactivar el bloqueo de acceso público de S3 en un bucket.

Gravedad predeterminada: baja

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que el bloqueo de acceso público se ha deshabilitado para el bucket de S3 que aparece en la lista. Cuando se activa, la configuración de Bloqueo de acceso público de S3 se utiliza para filtrar las políticas o las listas de control de acceso (ACL) aplicadas a los buckets como medida de seguridad para prevenir la exposición pública involuntaria de datos.

Normalmente, el Bloqueo de acceso público de S3 está desactivado en un bucket para permitir el acceso público a este o a los objetos que contiene. Cuando el Bloqueo de acceso público de S3 se deshabilita en un bucket, las políticas o las ACL que se han aplicado al bucket controlan el acceso a este. Esto no significa que el bucket se comparta públicamente, pero sí es importante auditar las políticas y ACL que se aplican al bucket para confirmar que se apliquen los permisos adecuados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Policy:S3/BucketPublicAccessGranted

Una entidad principal de IAM ha concedido acceso público a un bucket de S3 a todos los usuarios de AWS al cambiar las políticas o las ACL del bucket.

Gravedad predeterminada: alta

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que el bucket de S3 que aparece en la lista se ha expuesto públicamente a todos los usuarios de AWS autenticados porque una entidad de IAM ha cambiado una política de bucket o una ACL de ese bucket de S3.

Después de detectar un cambio de política o ACL, GuardDuty utiliza el razonamiento automatizado impulsado por [Zelkova](#) para determinar si el bucket es accesible públicamente.

 Note

Si las ACL o las políticas de un bucket están configuradas para denegar explícitamente o denegar todo, es posible que este resultado no refleje el estado actual del bucket. Este resultado no reflejará ninguna configuración de [Bloqueo de acceso público de S3](#) que pudiera haberse habilitado para su bucket de S3. En esos casos, el valor `effectivePermission` del resultado se marcará como UNKNOWN.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Stealth:S3/ServerAccessLoggingDisabled

El registro de acceso al servidor de S3 se ha deshabilitado para un bucket.

Gravedad predeterminada: baja

- Origen de datos: eventos de administración de CloudTrail

Este resultado le informa de que el registro de acceso al servidor de S3 está deshabilitado para un bucket dentro de su entorno de AWS. Si está deshabilitado, no se crea ningún registro de solicitud web de los intentos de acceso al bucket de S3 identificado; sin embargo, se siguen rastreando las llamadas a la API de administración de S3, como [DeleteBucket](#). Si el registro de eventos de datos de S3 está habilitado a través de CloudTrail para este bucket, se seguirá rastreando las solicitudes web para los objetos incluidos en el bucket. La desactivación del registro es una técnica que suelen utilizar los usuarios no autorizados para evitar que los detecten. Para obtener más información sobre los registros de S3, consulte [Registro de acceso al servidor de S3](#) y [Opciones de registro para S3](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Se ha invocado una API de S3 desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una operación de la API de S3, como PutObject o PutObjectAcl, desde una dirección IP que aparece en una lista de amenazas que ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

UnauthorizedAccess:S3/TorIPCaller

Se ha invocado una API de S3 desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que se ha invocado una operación de la API de S3, como PutObject o PutObjectAcl, desde una dirección IP de nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Este resultado puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Tipos de resultados de la protección de EKS

Los siguientes resultados son específicos de los recursos de Amazon EKS y tienen un `resource_type` de `EKSCluster`. La gravedad y los detalles de los resultados varían en función del tipo de resultado.

Para todos los resultados del tipo de registros de auditoría de EKS, recomendamos que examine el recurso en cuestión para determinar si la actividad es esperada o potencialmente maliciosa. Para obtener orientación sobre cómo corregir un recurso de registros de auditoría de EKS comprometido identificado por un resultado de GuardDuty, consulte [Corregir los resultados de EKS Protection](#).

Note

Si se espera la actividad por la que se generan estos resultados, considere agregar [Reglas de supresión en GuardDuty](#) para evitar futuras alertas.

Temas

- [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

Antes de la versión 1.14 de Kubernetes, el grupo `system:unauthenticated` estaba asociado a `system:discovery` y `system:basic-user`, que son ClusterRoles, de manera predeterminada. Esta asociación puede permitir el acceso no deseado de usuarios anónimos. Las actualizaciones del clúster no revocan estos permisos. Aunque se haya actualizado el clúster a la versión 1.14 o posterior, es posible que estos permisos sigan habilitados. Se recomienda que desasocie estos permisos del grupo

system:unauthenticated. Para obtener orientación sobre cómo revocar estos permisos, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se utiliza habitualmente para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP en una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoke los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoke el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

CredentialAccess:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos del clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para evadir medidas defensivas desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para evadir medidas de defensa desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La

API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para evadir medidas defensivas.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

DefenseEvasion:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para evadir medidas defensivas desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Discovery:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para descubrir recursos en un clúster de Kubernetes desde una dirección IP.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio.

 Para el acceso sin autenticar

Los resultados MaliciousIPCaller no se generan en caso de acceso sin autenticar.
Los resultados SuccessfulAnonymousAccess no se generan en caso de acceso sin autenticar o anónimo.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, invéstiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Discovery:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para detectar recursos en un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada se

suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoke los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoke el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Discovery:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para descubrir recursos en un clúster de Kubernetes.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a la fase de detección de un ataque, cuando un adversario recopila información sobre el clúster de Kubernetes. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Este tipo de resultado excluye los puntos de conexión de la API de comprobación de estado, como `/healthz`, `/livez`, `/readyz` y `/version`.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por

error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Discovery:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para detectar recursos en un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Execution:Kubernetes/ExecInKubeSystemPod

Se ha ejecutado un comando en un pod dentro del espacio de nombres **kube-system**

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado indica que se ha ejecutado un comando en un pod dentro del espacio de nombres kube-system mediante la API exec de Kubernetes. El espacio de nombres kube-system es un espacio de nombres predeterminado, que se utiliza principalmente para componentes de nivel de sistema, como kube-dns y kube-proxy. Es muy poco común ejecutar comandos dentro de pods o contenedores de un espacio de nombres kube-system, lo que puede indicar una actividad sospechosa.

Recomendaciones de corrección:

Si la ejecución de este comando es inesperada, es posible que las credenciales de identidad de usuario utilizada para ejecutar el comando se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Impact:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para manipular recursos en un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos de su entorno de AWS.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas](#)

[recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Impact:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos de su entorno de AWS.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Impact:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a la fase de impacto de un ataque, cuando un adversario está manipulando los recursos del clúster. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Impact:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos que están dentro de su entorno de AWS. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Persistence:Kubernetes/ContainerWithSensitiveMount

Se ha lanzado un contenedor con una ruta de host externa confidencial montada en su interior.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado indica que se ha lanzado un contenedor con una configuración que incluía una ruta de host confidencial con acceso de escritura en la sección `volumeMounts`. Esto hace que la ruta confidencial del host sea accesible y se pueda sobrescribir desde el interior del contenedor. Los adversarios suelen utilizar esta técnica para acceder al sistema de archivos del host.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de identidad de usuario utilizadas para lanzarlo se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si el lanzamiento de este contenedor es esperado, se recomienda utilizar una regla de supresión que consista en un criterio de filtrado basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe ser el mismo que el `imagePrefix` especificado en el resultado. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión](#).

Persistence:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para acceder a un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoke los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoke el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Persistence:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para obtener acceso persistente a un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este

resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Persistence:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para obtener permisos de nivel superior a un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster e intenta conservar ese acceso. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por

un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Persistence:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para acceder a un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoke los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoke el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Se concedieron privilegios de administrador en un clúster de Kubernetes a la cuenta de servicio predeterminada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se han concedido privilegios de administrador a la cuenta de servicio predeterminada de un espacio de nombres de su clúster de Kubernetes. Kubernetes crea una cuenta de servicio predeterminada para todos los espacios de nombres del clúster. Asigna automáticamente la cuenta de servicio predeterminada como identidad a los pods que no se han asociado explícitamente a otra cuenta de servicio. Si la cuenta de servicio predeterminada tiene privilegios de administrador, es posible que los pods se inicien involuntariamente con privilegios de administrador. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

No debe utilizar la cuenta de servicio predeterminada para conceder permisos a los pods. En su lugar, debe crear una cuenta de servicio dedicada para cada carga de trabajo y conceder el permiso a esa cuenta en función de sus necesidades. Para solucionar este problema, debe crear cuentas de servicio dedicadas para todos sus pods y cargas de trabajo, además de actualizar los pods y las cargas de trabajo para migrarlos de la cuenta de servicio predeterminada a sus cuentas dedicadas. A continuación, debe eliminar el permiso de administrador de la cuenta de servicio predeterminada. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Policy:Kubernetes/AnonymousAccessGranted

Se ha concedido un permiso de API al usuario **system:anonymous** en un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que un usuario de su clúster de Kubernetes ha creado correctamente un `ClusterRoleBinding` o `RoleBinding` para enlazar al usuario `system:anonymous` a un rol. Esto permite el acceso no autenticado a las operaciones de la API permitidas por el rol. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` o grupo `system:unauthenticated` en su clúster y revocar el acceso anónimo innecesario. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si los permisos se han concedido de forma maliciosa, debe revocar el acceso del usuario que concedió los permisos y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Policy:Kubernetes/ExposedDashboard

El panel de un clúster de Kubernetes estaba expuesto a Internet

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que el servicio de equilibrador de carga ha expuesto el panel de Kubernetes de su clúster a Internet. Un panel expuesto hace que la interfaz de administración del clúster sea accesible desde Internet y permite a los adversarios aprovechar cualquier brecha de autenticación y control de acceso que pueda existir.

Recomendaciones de corrección:

Debe asegurarse de que se apliquen una autenticación y una autorización sólidas en el panel de Kubernetes. También debe implementar un control de acceso a la red para restringir el acceso al panel desde direcciones IP específicas.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Policy:Kubernetes/KubeflowDashboardExposed

El panel de Kubeflow de un clúster de Kubernetes estaba expuesto a Internet

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que el servicio de equilibrador de carga ha expuesto el panel de Kubeflow de su clúster a Internet. Un panel de Kubeflow expuesto hace que la interfaz de administración del entorno de Kubeflow sea accesible desde Internet y permite a los adversarios aprovechar cualquier brecha de autenticación y control de acceso que pueda existir.

Recomendaciones de corrección:

Debe asegurarse de que se apliquen una autenticación y una autorización sólidas en el panel de Kubeflow. También debe implementar un control de acceso a la red para restringir el acceso al panel desde direcciones IP específicas.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Se ha lanzado un contenedor privilegiado con acceso a nivel raíz en su clúster de Kubernetes.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha lanzado un contenedor privilegiado en su clúster de Kubernetes mediante una imagen que nunca antes se había utilizado para lanzar contenedores privilegiados en su clúster. Un contenedor privilegiado tiene acceso de nivel raíz al host. Los adversarios pueden lanzar contenedores privilegiados como una táctica de derivación de privilegios para acceder al host y, posteriormente, ponerlo en peligro.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de identidad de usuario utilizadas para lanzarlo se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Se invocó de forma anómala una API de Kubernetes utilizada habitualmente para acceder a secretos.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado informa de que un usuario de Kubernetes del clúster ha invocado una operación anómala de la API para recuperar secretos confidenciales del clúster. La API observada normalmente se asocia con tácticas de acceso a credenciales que pueden conducir a una escalada de privilegios y a un mayor acceso dentro del clúster. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales de AWS están comprometidas.

La API observada fue identificada como anómala por el modelo de machine learning (ML) de detección de anomalías de GuardDuty. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de EKS e identifica eventos anómalos asociados a técnicas utilizadas por usuarios no autorizados. El modelo de ML hace un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó, el agente de usuario utilizado y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Examine los permisos concedidos al usuario de Kubernetes en el clúster y asegúrese de que todos estos permisos son necesarios. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Se creó o modificó un RoleBinding o ClusterRoleBinding a un rol demasiado permisivo o espacio de nombres confidencial en el clúster de Kubernetes.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si un RoleBinding o ClusterRoleBinding involucra los ClusterRoles `admin` o `cluster-admin`, la gravedad es alta.

- Característica: registros de auditoría de EKS

Este resultado informa de que un usuario en el clúster de Kubernetes ha creado un RoleBinding o ClusterRoleBinding para vincular un usuario a un rol con permisos de administrador o espacios de nombres confidenciales. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales de AWS están comprometidas.

La API observada fue identificada como anómala por el modelo de machine learning (ML) de detección de anomalías de GuardDuty. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. Además, el modelo de ML realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó, el agente de usuario utilizado y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Examine los permisos concedidos al usuario de Kubernetes. Estos permisos se definen en el rol y los sujetos implicados en RoleBinding y ClusterRoleBinding. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Se ejecutó un comando dentro de un pod de forma anómala.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado informa de que se ejecutó un comando en un pod mediante la API exec de Kubernetes. La API exec de Kubernetes permite ejecutar comandos arbitrarios en un pod. Si este comportamiento no es el esperado para el usuario, espacio de nombres o pod, puede ser indicio de un error de configuración o de que las credenciales de AWS están comprometidas.

La API observada fue identificada como anómala por el modelo de machine learning (ML) de detección de anomalías de GuardDuty. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. Además, el modelo de ML realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó, el agente de usuario utilizado y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Si la ejecución de este comando es inesperada, es posible que las credenciales de la identidad de usuario utilizada para ejecutar el comando se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Se lanzó una carga de trabajo con un contenedor privilegiado de forma anómala.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado informa de que se ha lanzado una carga de trabajo con un contenedor privilegiado en el clúster de Amazon EKS. Un contenedor privilegiado tiene acceso de nivel raíz al host. Los usuarios no autorizados pueden lanzar contenedores privilegiados como una táctica de escalada de privilegios para primero obtener acceso al host y luego comprometerlo.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty identificó como anómala la creación o modificación del contenedor observado. El modelo de ML evalúa toda la actividad de la API del usuario y de la imagen del contenedor dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Si este lanzamiento de contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Si este lanzamiento de contenedor está previsto, se recomienda utilizar una regla de supresión con un criterio de filtro basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe tener el mismo valor que el campo `imagePrefix` especificado en el resultado. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

**Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!
ContainerWithSensitiveMount**

Se implementó una carga de trabajo de forma anómala, con una ruta de host confidencial montada dentro de la carga de trabajo.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado informa de que se ha lanzado una carga de trabajo con un contenedor que incluía una ruta de host confidencial en la sección `volumeMounts`. Esto potencialmente hace que la ruta confidencial del host sea accesible y que se pueda escribir en esta desde dentro del contenedor. Esta técnica es comúnmente utilizada por usuarios no autorizados para obtener acceso al sistema de archivos del host.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty identificó como anómala la creación o modificación del contenedor observado. El modelo de ML evalúa toda la actividad de la API del usuario y de la imagen del contenedor dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Si este lanzamiento de contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Si este lanzamiento de contenedor está previsto, se recomienda utilizar una regla de supresión con un criterio de filtro basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe tener el mismo valor que el campo `imagePrefix` especificado en el resultado. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Se lanzó una carga de trabajo de forma anómala.

Gravedad predeterminada: baja*

Note

La gravedad predeterminada es Baja. Sin embargo, si la carga de trabajo contiene un nombre de imagen potencialmente sospechoso, como una herramienta de prueba de penetración conocida, o un contenedor que ejecuta un comando potencialmente sospechoso al momento del lanzamiento, como comandos de intérprete de comandos inverso, entonces la gravedad de este tipo de resultado se considerará Media.

- Característica: registros de auditoría de EKS

Este resultado informa de que se ha creado o modificado una carga de trabajo de Kubernetes de forma anómala, como una actividad de la API, nuevas imágenes de contenedor o una configuración arriesgada de la carga de trabajo, dentro del clúster de Amazon EKS. Los usuarios no autorizados pueden lanzar contenedores como una táctica para ejecutar código arbitrario para primero obtener acceso al host y luego comprometerlo.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty identificó como anómala la creación o modificación del contenedor observado. El modelo de ML evalúa toda la actividad de la API del usuario y de la imagen del contenedor dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Si este lanzamiento de contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Si este lanzamiento de contenedor está previsto, se recomienda utilizar una regla de supresión con un criterio de filtro basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe tener el mismo valor que el campo `imagePrefix` especificado en el resultado. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Se ha creado o modificado de forma anómala un Role o ClusterRole altamente permisivo.

Gravedad predeterminada: baja

- Característica: registros de auditoría de EKS

Este resultado informa de que un usuario de Kubernetes en el clúster de Amazon EKS ha llamado a una operación de la API anómala para crear un Role o ClusterRole con permisos excesivos. Los actores pueden utilizar la creación de roles con permisos elevados para evitar el uso de roles predefinidos similares a administradores y evadir la detección. El exceso de permisos puede derivar en la escalada de privilegios, la ejecución remota de código e incluso el control completo de un espacio de nombres o clúster. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales están comprometidas.

La API observada fue identificada como anómala por el modelo de machine learning (ML) de detección de anomalías de GuardDuty. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de Amazon EKS e identifica eventos anómalos asociados a las técnicas utilizadas por usuarios no autorizados. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Examine los permisos definidos en `Role` o `ClusterRole` para asegurarse de que todos los permisos son necesarios y siguen los principios de mínimo privilegio. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un usuario comprobó su permiso de acceso de forma anómala.

Gravedad predeterminada: baja

- Característica: registros de auditoría de EKS

Este resultado indica que un usuario en el clúster de Kubernetes ha verificado con éxito si están habilitados permisos elevados conocidos, los cuales pueden facilitar la escalada de privilegios y la ejecución remota de código. Por ejemplo, `kubectl auth can-i` es un comando común utilizado para comprobar los permisos de un usuario. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales se han visto comprometidas.

La API observada fue identificada como anómala por el modelo de machine learning (ML) de detección de anomalías de GuardDuty. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de Amazon EKS e identifica eventos anómalos asociados a las técnicas utilizadas por usuarios no autorizados. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el permiso que se comprueba y el espacio de nombres que el usuario operó. Puede encontrar los detalles de la solicitud de la API que resultan inusuales en el panel de detalles del resultado en la consola de GuardDuty.

Recomendaciones de corrección:

Examine los permisos concedidos al usuario de Kubernetes para asegurarse de que todos los permisos son necesarios. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si las credenciales de AWS están comprometidas, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty

Amazon GuardDuty genera los siguientes resultados de supervisión en tiempo de ejecución para indicar posibles amenazas basadas en el comportamiento a nivel del sistema operativo de los hosts y contenedores de Amazon EC2 en los clústeres de Amazon EKS, cargas de trabajo de Fargate y Amazon ECS e instancias de Amazon EC2.

Note

Los tipos de resultados de la Supervisión en tiempo de ejecución se obtienen según los registros de tiempo de ejecución recopilados de los hosts. Los registros contienen campos, como las rutas de los archivos, que puede controlar un agente malicioso. Estos campos también se incluyen en los resultados de GuardDuty para proporcionar un contexto de tiempo de ejecución. Al procesar los resultados de la Supervisión en tiempo de ejecución fuera de la consola de GuardDuty, debe sanear los campos de resultado. Por ejemplo, puede codificar en HTML los campos de resultado cuando los muestre en una página web.

Temas

- [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

Una instancia o un contenedor de Amazon EC2 está consultando una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se estaba ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con una actividad relacionada con criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si utiliza esta instancia o un contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado CryptoCurrency:Runtime/BitcoinTool.B podría representar la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de CryptoCurrency:Runtime/BitcoinTool.B. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad relacionada con las criptomonedas o las cadenas de bloques. Para obtener más información, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Backdoor:Runtime/C&CActivity.B

Una instancia o un contenedor de Amazon EC2 está consultando una IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 mostrados en el entorno de AWS consultan una dirección IP asociada a un servidor de comando y control (C&C) conocido. La instancia o el contenedor que aparecen en la lista podrían estar potencialmente afectados. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

Note

Si la IP consultada está relacionada con log4j, los campos del resultado asociado incluirán los siguientes valores:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

UnauthorizedAccess:Runtime/TorRelay

La instancia o contenedor de Amazon EC2 está estableciendo conexiones a una red de Tor como relé de Tor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 de su entorno de AWS está estableciendo conexiones con una red de Tor de una forma que sugiere que actúa como un relé de Tor. Tor es un software que permite la comunicación anónima. Tor incrementa el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

UnauthorizedAccess:Runtime/TorClient

La instancia o el contenedor de Amazon EC2 está estableciendo conexiones con un nodo Authority o Guard de Tor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 del entorno de AWS está estableciendo conexiones con un nodo Authority o Guard de Tor. Tor es un software que permite la comunicación anónima. Los nodos Guard y Authority de Tor actúan como puertas de enlace a una red de Tor. Este tráfico puede indicar que esta instancia o el contenedor de EC2 se han visto afectados y están actuando como clientes en una red de Tor. Este resultado puede significar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/BlackholeTraffic

Una instancia o un contenedor de Amazon EC2 intenta comunicarse con una dirección IP de un host remoto que es un agujero negro conocido.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectado, ya que está intentando comunicarse con una dirección IP de agujero negro (u oculta). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/DropPoint

Una instancia o un contenedor de Amazon EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 de su entorno de AWS está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio asociado con una actividad de criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de los recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si utiliza esta instancia o contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado `CryptoCurrency:Runtime/BitcoinTool.B!DNS` podría representar la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtrado. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad de criptomonedas o cadenas de bloques. Para obtener más información, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Backdoor:Runtime/C&CActivity.B!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio que está asociado a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La instancia o el contenedor de EC2 de la lista podrían haberse visto afectados. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

Note

Si el nombre de dominio consultado está relacionado con log4j, los campos del resultado asociado incluirán los siguientes valores:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

Note

Para probar cómo GuardDuty genera este tipo de resultado, puede hacer una solicitud de DNS desde su instancia (mediante `dig` para Linux o `nslookup` para Windows) a un dominio de prueba `guarddutyec2activityb.com`.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/BlackholeTraffic!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectado, ya que está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro. Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/DropPoint!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de un host remoto que se conoce que conservar credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 de su entorno de AWS está consultando un nombre de dominio de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/DGADomainRequest.C!DNS

Una instancia o un contenedor de Amazon EC2 está consultando dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar que una instancia o un contenedor de EC2 se han visto afectados.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está intentando consultar dominios de algoritmos de generación de dominios (DGA). Es posible que su recurso se haya visto afectado.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C&C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

Note

Este resultado se basa en dominios DGA conocidos de las fuentes de información de amenazas de GuardDuty.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/DriveBySourceTraffic!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de un host remoto que es una fuente conocida de ataques de descarga Drive-By.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio de un host remoto que es un origen conocido de ataques de descargas Drive-By. Se trata de descargas no deseadas de software informático desde Internet que pueden iniciar la instalación automática de un virus, spyware o malware.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Trojan:Runtime/PhishingDomainRequest!DNS

Una instancia o un contenedor de Amazon EC2 está consultando dominios implicados en ataques de suplantación de identidad.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 en el entorno de AWS está intentando consultar un dominio implicado en ataques de suplantación de identidad. Los dominios de suplantación de identidad los configura alguien que se presenta como una institución legítima para inducir a las personas a proporcionar información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas. Es posible que su instancia o contenedor de EC2 esté intentando recuperar datos confidenciales almacenados en un sitio web de suplantación de identidad o que esté intentando configurar un sitio web de este tipo. Su instancia o contenedor de EC2 podrían haberse visto afectados.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Impact:Runtime/AbusedDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a dominios que se sabe que se han utilizado indebidamente.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que se ha utilizado indebidamente. Algunos ejemplos de dominios utilizados indebidamente son los nombres de dominio de nivel superior (TLD) y los nombres de dominio de segundo nivel (2LD), que proporcionan registros de subdominios gratuitos, así como proveedores de DNS dinámicos. Los actores de amenazas suelen utilizar estos servicios para registrar dominios de forma gratuita o a un bajo costo. Los dominios de baja reputación de esta categoría también pueden ser dominios caducados que se resuelven en la dirección IP de estacionamiento de un registrador y, por lo tanto, es posible que ya no estén activos. Una IP de estacionamiento es el lugar al que un registrador dirige el tráfico de dominios que no se han vinculado a ningún servicio. La instancia o el contenedor de Amazon EC2 que aparece en la lista pueden haberse visto afectados, ya que los actores de amenazas suelen utilizar estos registradores o servicios para la distribución de C&C y malware.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Impact:Runtime/BitcoinDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a la actividad relacionada con la criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio que está asociado a actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si utiliza esta instancia o el contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado podría representar la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `Impact:Runtime/BitcoinDomainRequest.Reputation`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad relacionada con las criptomonedas o las cadenas de bloques. Para obtener más información, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Impact:Runtime/MaliciousDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a dominios maliciosos conocidos.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP maliciosos conocidos. Por ejemplo, los dominios pueden estar asociados a una dirección IP conocida como oculta. Los dominios ocultos son aquellos que anteriormente estaban controlados por un agente de amenazas y las solicitudes que se les hagan pueden indicar que la instancia se ha visto afectada. Estos dominios también pueden estar correlacionados con campañas o algoritmos de generación de dominios maliciosos conocidos.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Impact:Runtime/SuspiciousDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que resulta sospechoso por naturaleza debido a su antigüedad o a su baja popularidad.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación que se sospecha puede ser malicioso. Las características observadas de este dominio coincidían con las de los dominios maliciosos observados anteriormente. Sin embargo, nuestro modelo de reputación no pudo relacionarlo definitivamente con una amenaza conocida. Por lo general, estos dominios se han detectado recientemente o reciben poco tráfico.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

UnauthorizedAccess:Runtime/MetadataDNSRebind

Una instancia o un contenedor de Amazon EC2 hace búsquedas de DNS que se resuelven en el servicio de metadatos de instancia.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Note

Actualmente, este tipo de resultados solo se admite para la arquitectura AMD64.

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 del entorno de AWS está consultando un dominio que se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Una consulta de DNS de este tipo puede indicar que la instancia es el objetivo de una técnica de reenlace de DNS. Esta técnica se puede utilizar para obtener metadatos de una instancia de EC2, que incluye las credenciales de IAM asociadas a la instancia.

El reenlace de DNS implica engañar a una aplicación que se ejecuta en la instancia de EC2 para que cargue datos devueltos desde una URL, de tal forma que el nombre de dominio de la URL se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Esto hace que la aplicación obtenga acceso a los metadatos de EC2 y, posiblemente, los ponga a disposición del atacante.

Solo se puede obtener acceso a los metadatos de EC2 mediante el reenlace de DNS si la instancia de EC2 ejecuta una aplicación vulnerable que permite la inserción de URL o si un usuario obtiene acceso a la URL en un navegador web que se ejecuta en la instancia de EC2.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

En respuesta a este resultado, es importante evaluar si hay alguna aplicación vulnerable que se esté ejecutando en la instancia o en el contenedor de EC2 o si un usuario ha utilizado un navegador para acceder al dominio identificado en el resultado. Si la causa raíz es una aplicación vulnerable, corrija la vulnerabilidad. Si un usuario ha navegado por el dominio identificado, bloquee el dominio o impida que los usuarios puedan acceder a él. Si determina que el resultado está relacionado con cualquiera de los casos anteriores, debe [revocar la sesión asociada a la instancia de EC2](#).

Algunos clientes de AWS asignan deliberadamente la dirección IP de metadatos a un nombre de dominio en sus servidores DNS autorizados. Si este es el caso en su entorno de , le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. El segundo criterio de filtro debe ser el Dominio de la solicitud de DNS o el ID de imagen de contenedor del contenedor. El valor Dominio de la solicitud DNS debe coincidir con el dominio que ha asignado a la dirección IP de metadatos (169.254.169.254). Para obtener información sobre la creación de reglas de supresión, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/NewBinaryExecuted

Se ha ejecutado un archivo binario recién creado o que se ha modificado recientemente en un contenedor.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado un archivo binario recién creado o modificado en un contenedor. Se recomienda mantener los contenedores inmutables durante el tiempo de ejecución y los archivos binarios, scripts o bibliotecas no deben crearse ni modificarse durante la vida útil del contenedor. Este comportamiento indica que un actor malicioso que ha obtenido acceso al contenedor ha descargado y ejecutado malware u otro software como parte del comprometimiento potencial. Aunque este tipo de actividad podría ser un indicio de un comprometimiento, también se trata de un patrón de uso habitual. Por lo tanto, GuardDuty utiliza mecanismos para identificar instancias sospechosas de esta actividad y genera este tipo de resultado únicamente para instancias sospechosas.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. Para identificar el proceso de modificación y el nuevo binario, consulte los detalles del Proceso de modificación y los detalles del Proceso

Los detalles del proceso de modificación se incluyen en el campo `service.runtimeDetails.context.modifyingProcess` del JSON del resultado, o en Proceso de modificación en el panel de detalles del resultado. Para este tipo de resultado, el proceso de modificación es `/usr/bin/dpkg`, como se identifica en el campo `service.runtimeDetails.context.modifyingProcess.executablePath` del JSON del resultado, o como parte del Proceso de modificación en el panel de detalles del resultado.

Los detalles del binario nuevo o modificado ejecutado se incluyen en el `service.runtimeDetails.process` del JSON del resultado, o en la sección Proceso bajo Detalles de tiempo de ejecución. Para este tipo de resultado, el binario nuevo o modificado es `/usr/bin/python3.8`, como se indica en el campo `service.runtimeDetails.process.executablePath` (Ruta ejecutable).

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un proceso dentro de un contenedor se comunica con el daemon de Docker mediante un socket de Docker.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

El socket de Docker es un socket de dominio Unix que el daemon de Docker (dockerd) utiliza para comunicarse con sus clientes. Un cliente puede llevar a cabo diversas acciones, como crear contenedores al comunicarse con el daemon de Docker a través del socket de Docker. Es sospechoso que un proceso de contenedor acceda al socket de Docker. Un proceso de contenedor puede escapar del contenedor y obtener acceso de host al comunicarse con el socket de Docker y crear un contenedor privilegiado.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/RuncContainerEscape

Se detectó un intento de escape del contenedor a través de runC.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

RunC es el tiempo de ejecución de contenedores de bajo nivel que los tiempos de ejecución de contenedores de alto nivel, como Docker y Containerd utilizan para generar y ejecutar contenedores. RunC siempre se ejecuta con privilegios de raíz porque necesita realizar la tarea de bajo nivel de crear un contenedor. Un actor que represente una amenaza puede obtener acceso a nivel de host ya sea al modificar o explotar una vulnerabilidad en el binario de runC.

Este resultado detecta la modificación del binario de runC y posibles intentos de explotar las siguientes vulnerabilidades de runC:

- [CVE-2019-5736](#): la explotación de CVE-2019-5736 implica sobrescribir el binario de runC desde dentro de un contenedor. Este resultado se invoca cuando un proceso dentro de un contenedor modifica el binario de runC.
- [CVE-2024-21626](#): la explotación de CVE-2024-21626 implica establecer el directorio de trabajo actual (CWD) o un contenedor en un descriptor de archivo abierto `/proc/self/fd/FileDescriptor`. Este resultado se invoca cuando se detecta un proceso de contenedor con un directorio de trabajo actual bajo `/proc/self/fd/`, por ejemplo, `/proc/self/fd/7`.

Este resultado puede indicar que un actor malicioso ha intentado realizar una explotación en uno de los siguientes tipos de contenedores:

- Un contenedor nuevo con una imagen controlada por un atacante.
- Un contenedor existente al que el actor tenía acceso con permisos de escritura en el binario de runC a nivel de host.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Se detectó un intento de escape de un contenedor a través del agente de liberación de CGroups.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha detectado un intento de modificar el archivo de agente de lanzamiento de un grupo de control (cgroup). Linux utiliza grupos de control (cgroups) para limitar, contabilizar y aislar el uso de recursos de un conjunto de procesos. Cada cgroup tiene un archivo de agente de lanzamiento (`release_agent`), un script que Linux ejecuta cuando termina cualquier

proceso dentro del cgroup. El archivo de agente de lanzamiento debe ejecutarse siempre en el host. Un actor de amenazas dentro de un contenedor puede escapar al host mediante la escritura de comandos arbitrarios en el archivo de agente de lanzamiento que pertenece a un cgroup. Cuando termina un proceso dentro de ese cgroup, se ejecutan los comandos escritos por el actor.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/ProcessInjection.Proc

Se ha detectado una inyección de proceso mediante el sistema de archivos proc en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. El sistema de archivos proc (procfs) es un sistema de archivos especial de Linux que presenta la memoria virtual del proceso como un archivo. La ruta de ese archivo es `/proc/PID/mem`, donde PID es el ID único del proceso. Un actor de amenazas puede escribir en este archivo para inyectar código en el proceso. Este resultado identifica los posibles intentos de escritura en este archivo.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Se ha detectado una inyección de proceso mediante una llamada al sistema ptrace en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. Un proceso puede utilizar la llamada al sistema ptrace para inyectar código en otro proceso. Este resultado identifica un posible intento de inyectar código en un proceso mediante la llamada al sistema ptrace.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Se ha detectado una inyección de proceso mediante una escritura directa en la memoria virtual en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. Un proceso puede utilizar una llamada al sistema como `process_vm_writev` para inyectar código directamente

en la memoria virtual de otro proceso. Este resultado identifica un posible intento de inyectar código en un proceso mediante la llamada al sistema para escribir en la memoria virtual del proceso.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/ReverseShell

Un proceso en un contenedor o en una instancia de Amazon EC2 ha creado un intérprete de comandos inverso.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Un intérprete de comandos inverso es una sesión de intérprete de comandos que se crea en una conexión que se ha iniciado del host de destino al host del actor. Esto es lo opuesto a un intérprete de comandos normal que se inicia desde el host del actor hasta el host de destino. Los actores de amenazas crean un intérprete de comandos inverso para ejecutar comandos en el objetivo tras obtener el acceso inicial a este. Este resultado identifica conexiones de intérprete de comandos inverso que son potencialmente sospechosas.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, y genera este tipo de resultado solo cuando la actividad y el contexto asociados se descubre que son inusuales o sospechosos. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

El agente de GuardDuty monitorea eventos de múltiples orígenes. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. Si

esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/FilelessExecution

Un proceso en un contenedor o en una instancia de Amazon EC2 ejecuta código desde la memoria.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa cuando se ejecuta un proceso mediante un archivo ejecutable en memoria en el disco. Se trata de una técnica de evasión de defensa habitual que impide escribir el ejecutable malicioso en el disco para evitar la detección basada en el análisis del sistema de archivos. Si bien el malware utiliza esta técnica, también tiene algunos casos de uso legítimos. Uno de los ejemplos es un compilador Just-in-time (JIT) que escribe código compilado en la memoria y lo ejecuta desde ahí.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Impact:Runtime/CryptoMinerExecuted

Una instancia o un contenedor de Amazon EC2 ejecuta un archivo binario asociado con una actividad de extracción de criptomonedas.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 del entorno de AWS está ejecutando un archivo binario que está asociado con una actividad de extracción de criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente afectado, consulte el Tipo de recurso en el panel de resultados de la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty y consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/NewLibraryLoaded

Un proceso ha cargado una biblioteca recién creada o modificada recientemente dentro de un contenedor.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha creado una biblioteca o que esta se ha modificado dentro de un contenedor durante el tiempo de ejecución y que un proceso que se ejecuta dentro del contenedor la ha cargado. Se recomienda mantener los contenedores inmutables durante el tiempo de ejecución y los archivos binarios, scripts o bibliotecas no deben crearse ni modificarse durante la vida útil del contenedor. La carga de una biblioteca recién creada o modificada en un contenedor puede indicar actividad sospechosa. Este comportamiento indica la posibilidad de que un actor malicioso haya accedido al contenedor, haya descargado y ejecutado malware u otro software como parte de una posible amenaza. Aunque este tipo de actividad podría ser un indicio de un comprometimiento, también se trata de un patrón de uso habitual. Por lo tanto, GuardDuty utiliza mecanismos para identificar instancias sospechosas de esta actividad y genera este tipo de resultado únicamente para instancias sospechosas.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un proceso dentro de un contenedor ha montado un sistema de archivos de host durante el tiempo de ejecución.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Varias técnicas de escape de contenedores implican montar un sistema de archivos de host dentro de un contenedor durante el tiempo de ejecución. Este resultado indica que un proceso dentro de un contenedor podría intentar montar un sistema de archivos de host, lo que podría indicar un intento de escape al host.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un proceso ha utilizado llamadas al sistema **userfaultfd** para gestionar los errores de página en el espacio de usuario.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Por lo general, los errores de página los gestiona el kernel en el espacio del kernel. Sin embargo, la llamada al sistema `userfaultfd` permite que un proceso gestione los errores de página en un sistema de archivos del espacio de usuario. Esta es una característica útil que permite la implementación de sistemas de archivos en el espacio de usuario. Por otro lado, también puede ser utilizada por un proceso potencialmente malicioso para interrumpir el funcionamiento del kernel desde el espacio de usuario. Interrumpir el kernel mediante una llamada al sistema `userfaultfd` es una técnica de explotación común para ampliar los intervalos de carrera cuando se explotan las condiciones de carrera del kernel. El uso de `userfaultfd` puede indicar una actividad sospechosa en la instancia de Amazon Elastic Compute Cloud (Amazon EC2).

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/SuspiciousTool

Un contenedor o una instancia de Amazon EC2 está ejecutando un archivo binario o un script que se utiliza con frecuencia en escenarios de seguridad ofensiva, como pruebas de penetración.

Gravedad predeterminada: variable

La gravedad de este resultado puede ser alta o baja, según si la herramienta sospechosa detectada se considera de doble uso o es de uso exclusivamente ofensivo.

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado una herramienta sospechosa en una instancia de EC2 o en un contenedor del entorno de AWS. Esto incluye las herramientas utilizadas en las actividades de pruebas de penetración, también conocidas como herramientas de puerta trasera, analizadores de red y rastreadores de red. Todas estas herramientas se pueden utilizar en contextos benignos, pero también las utilizan con frecuencia los actores de amenazas con intenciones maliciosas. Si se observan herramientas de seguridad ofensivas, podría ser un indicio de que la instancia de EC2 o el contenedor asociados se han visto comprometidos.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, por lo que únicamente genera este resultado cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o un contenedor que es indicativo de un comprometimiento.

Gravedad predeterminada: variable

Según el impacto del patrón malicioso observado, la gravedad de este tipo de resultado podría ser baja, media o alta.

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado un comando sospechoso e indica que una instancia de Amazon EC2 o un contenedor del entorno de AWS se han visto comprometidos. Esto puede significar que se ha descargado un archivo de una fuente sospechosa y luego se ha ejecutado, o que un proceso en ejecución muestra un patrón malicioso conocido en su línea de comandos. Esto indica además la presencia de malware en ejecución en el sistema.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, por lo que únicamente genera este resultado cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/SuspiciousCommand

Se ha ejecutado un comando en la instancia de Amazon EC2 o en un contenedor de la lista, intenta modificar o desactivar un mecanismo de defensa de Linux, como el firewall o los servicios esenciales del sistema.

Gravedad predeterminada: variable

Según el mecanismo de defensa que se haya modificado o desactivado, la gravedad de este tipo de resultado puede ser alta, media o baja.

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado un comando que intenta ocultar un ataque a los servicios de seguridad del sistema local. Esto incluye acciones como desactivar el firewall de Unix, modificar las tablas de IP locales, eliminar entradas crontab, desactivar un servicio local o asumir la función de LDPreload. Cualquier modificación es altamente sospechosa y un indicador potencial de comprometimiento. Por lo tanto, estos mecanismos detectan que el sistema está comprometido o impiden que se comprometa aún más.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, por lo que únicamente genera este resultado cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso potencialmente comprometido, consulte Tipo de recurso en los detalles de los resultados en la Consola de GuardDuty. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/PtraceAntiDebugging

Un proceso en un contenedor o una instancia de Amazon EC2 ha ejecutado una medida antidepuración mediante la llamada al sistema ptrace.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este resultado muestra que un proceso que se ejecuta en la instancia de Amazon EC2 que se encuentra en la lista o un contenedor dentro del entorno de AWS ha utilizado la llamada al sistema ptrace con la opción PTRACE_TRACEME. Esta actividad provocaría que un depurador asociado se separara del proceso en ejecución. Si no hay ningún depurador asociado, no se producirá ningún efecto. Sin embargo, la actividad en sí misma suscita sospechas. Esto podría ser indicio de la presencia de malware en ejecución en el sistema. El malware utiliza con frecuencia técnicas antidepuración para eludir los análisis, y estas técnicas se pueden detectar en tiempo de ejecución.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, por lo que únicamente genera este resultado cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/MaliciousFileExecuted

Se ha ejecutado un archivo ejecutable malicioso conocido en una instancia de Amazon EC2 o en un contenedor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado un ejecutable malicioso conocido en una instancia de Amazon EC2 o en un contenedor del entorno de AWS. Se trata de un sólido indicio de que la instancia o el contenedor se han visto potencialmente comprometidos y de que se ha ejecutado malware.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, por lo que únicamente genera este resultado cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Execution:Runtime/SuspiciousShellCreated

Un servicio de red o un proceso al que se puede acceder a través de la red en una instancia de Amazon EC2 o en un contenedor ha iniciado un proceso de intérprete de comandos interactivo.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que un servicio al que se puede acceder a través de la red en una instancia de Amazon EC2 o en un contenedor del entorno de AWS ha iniciado un intérprete de comandos interactivo. En determinadas circunstancias, este escenario podría ser indicio de un comportamiento posterior a la explotación. Los intérpretes de comandos interactivos permiten a los atacantes ejecutar comandos arbitrarios en una instancia o contenedor comprometidos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación. Puede ver la información del proceso al que se puede acceder a través de la red en los detalles del proceso principal.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/ElevationToRoot

Un proceso que se ejecuta en la instancia o contenedor de Amazon EC2 que aparece en la lista ha asumido privilegios de raíz.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que un proceso que se ejecuta en el Amazon EC2 de la lista o en el contenedor de la lista dentro del entorno de `setuid` ha asumido privilegios de raíz a través de una ejecución binaria AWS inusual o sospechosa. Esto indica que un proceso en ejecución ha sido potencialmente comprometido, para la instancia de EC2 a través de un exploit, o a través de la explotación `setuid`. Al utilizar los privilegios de raíz, el atacante puede potencialmente ejecutar comandos en la instancia o el contenedor.

A pesar de que GuardDuty se diseñó para no generar este tipo de resultados en el caso de actividades que involucren el uso habitual del comando `sudo`, generará este resultado cuando identifique la actividad como inusual o sospechosa.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, y genera este tipo de resultado solo cuando la actividad y el contexto asociados son inusuales o sospechosos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Discovery:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor, lo que permite a un atacante obtener información sobre el sistema local, la infraestructura de AWS circundante o la infraestructura del contenedor.

Gravedad predeterminada: baja

Característica: supervisión en tiempo de ejecución

Este resultado informa de que un proceso que se está ejecutando en la instancia o contenedor de Amazon EC2 listados en el entorno de AWS han ejecutado un comando que podría proporcionar información crucial a un atacante para posibles avances en su cometido. Es posible que se haya recuperado la siguiente información:

- Sistema local, como la configuración del usuario o de la red,
- Otros recursos y permisos de AWS disponibles, o
- Infraestructura de Kubernetes, como servicios y pods.

Es posible que la instancia de Amazon EC2 o el contenedor que aparece en los detalles del resultado se hayan visto comprometidos.

El agente de tiempo de ejecución de GuardDuty supervisa eventos de múltiples tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte Tipo de recurso en los detalles de los resultados en la Consola de GuardDuty. Puede encontrar los detalles sobre el comando sospechoso en el campo `service.runtimeDetails.context` del JSON del resultado. El

contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Persistence:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor, lo que permite a un atacante persistir en el acceso y el control en el entorno de AWS.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que un proceso que se está ejecutando en una instancia de Amazon EC2 o en un contenedor del entorno de AWS ha ejecutado un comando sospechoso. El comando instala un método de persistencia que permite al malware ejecutarse ininterrumpidamente, o permite a un atacante acceder continuamente al tipo de recurso de instancia o contenedor potencialmente comprometido. Esto podría significar que se ha instalado o modificado un servicio del sistema, se ha modificado el `crontab` o se ha añadido un nuevo usuario a la configuración del sistema.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, y genera este tipo de resultado solo cuando la actividad y el contexto asociados son inusuales o sospechosos.

Es posible que la instancia de Amazon EC2 o el contenedor que aparece en los detalles del resultado se hayan visto comprometidos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso potencialmente comprometido, consulte Tipo de recurso en los detalles de los resultados en la Consola de GuardDuty. Puede encontrar los detalles sobre el comando sospechoso en el campo `service.runtimeDetails.context` del JSON del resultado. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

PrivilegeEscalation:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor, lo cual permite a un atacante escalar privilegios.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que un proceso que se está ejecutando en una instancia de Amazon EC2 o en un contenedor del entorno de AWS ha ejecutado un comando sospechoso. El comando intenta realizar una escalada de privilegios, lo que permite a un adversario realizar tareas de alto privilegio.

GuardDuty examina la actividad en tiempo de ejecución y el contexto relacionados, y genera este tipo de resultado solo cuando la actividad y el contexto asociados son inusuales o sospechosos.

Es posible que la instancia de Amazon EC2 o el contenedor que aparece en los detalles del resultado se hayan visto comprometidos.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

DefenseEvasion:Runtime/KernelModuleLoaded

Se cargó un módulo de núcleo en una instancia de Amazon EC2, lo que indica un intento de obtener acceso a nivel de núcleo.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado indica que se cargó un módulo del núcleo en la instancia de EC2 mostrada. Dado que los módulos del núcleo tienen los privilegios más altos por sistema (anillo 0), esto podría indicar que un agente de amenazas ha obtenido acceso del núcleo. Este nivel de acceso permite un control total del sistema.

El agente en tiempo de ejecución de GuardDuty supervisa eventos de múltiples recursos. Para identificar el recurso afectado, consulte Tipo de recurso en los detalles de los resultados en la consola de GuardDuty. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

Tipos de resultados de la protección contra malware para EC2

La protección contra malware de GuardDuty para EC2 proporciona un único resultado de protección contra malware para EC2 para todas las amenazas detectadas durante el análisis de una instancia de EC2 o una carga de trabajo de contenedor. El resultado incluye el número total de detecciones hechas durante el análisis y, en función de la gravedad, proporciona detalles sobre las 32 amenazas principales que detecta. A diferencia de otros resultados de GuardDuty, los resultados de la protección contra malware para EC2 no se actualizan cuando se vuelve a analizar la misma instancia de EC2 o la misma carga de trabajo de contenedor.

Se genera un nuevo resultado de protección contra malware para EC2 por cada análisis que detecta malware. Los resultados de la protección contra malware para EC2 incluyen información sobre el análisis correspondiente que produjo el resultado, así como el resultado de GuardDuty que inició este análisis. Esto facilita la correlación entre el comportamiento sospechoso y el malware detectado.

Note

Cuando GuardDuty detecta actividad maliciosa en una carga de trabajo de contenedor, la protección contra malware para EC2 no genera un resultado de nivel EC2.

Los siguientes resultados son específicos de la protección contra malware de GuardDuty para EC2.

Temas

- [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

Se ha detectado un archivo malicioso en una instancia de EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos maliciosos en la instancia de EC2 que aparece en la lista en el entorno de AWS. La instancia que aparece en la lista podría haberse visto afectada. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Execution:ECS/MaliciousFile

Se ha detectado un archivo malicioso en un clúster de ECS.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor que pertenece a un clúster de ECS. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el contenedor que pertenece al clúster de ECS se haya visto afectado. Para obtener más información, consulte [Corregir un clúster de ECS potencialmente comprometido](#).

Execution:Kubernetes/MaliciousFile

Se ha detectado un archivo malicioso en un clúster de Kubernetes.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor que pertenece a un clúster de Kubernetes. Si se trata de un clúster administrado por EKS, los detalles de los resultados proporcionarán información adicional sobre el recurso de EKS afectado. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Execution:Container/MaliciousFile

Se ha detectado un archivo malicioso en un contenedor independiente.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor y no se ha identificado información sobre el clúster. Para obtener más información, consulte la sección **Amenazas detectadas** en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir un contenedor independiente potencialmente comprometido](#).

Execution:EC2/SuspiciousFile

Se ha detectado un archivo sospechoso en una instancia de EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos sospechosos en una instancia de EC2. Para obtener más información, consulte la sección **Amenazas detectadas** en los detalles de los resultados.

Las detecciones de tipo **SuspiciousFile** indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se haya detectado un archivo sospechoso, evalúe si espera verlo en su entorno de AWS. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Execution:ECS/SuspiciousFile

Se ha detectado un archivo sospechoso en un clúster de ECS.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos sospechosos en un contenedor que pertenece a un clúster de ECS. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se haya detectado un archivo sospechoso, evalúe si espera verlo en su entorno de AWS. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el contenedor que pertenece al clúster de ECS se haya visto afectado. Para obtener más información, consulte [Corregir un clúster de ECS potencialmente comprometido](#).

Execution:Kubernetes/SuspiciousFile

Se ha detectado un archivo sospechoso en un clúster de Kubernetes.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos sospechosos en un contenedor que pertenece a un clúster de Kubernetes. Si se trata de un clúster administrado por EKS, los detalles de los resultados proporcionarán información adicional sobre el EKS afectado. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se haya detectado un archivo sospechoso, evalúe si espera verlo en su entorno de AWS. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Execution:Container/SuspiciousFile

Se ha detectado un archivo sospechoso en un contenedor independiente.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de la protección contra malware de GuardDuty para EC2 ha detectado uno o más archivos sospechosos en un contenedor sin información de clúster. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos

programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se haya detectado un archivo sospechoso, evalúe si espera verlo en su entorno de AWS. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir un contenedor independiente potencialmente comprometido](#).

Tipo de resultado de la protección contra malware para S3

GuardDuty genera un resultado solo cuando detecta una amenaza potencial a la seguridad en la Cuenta de AWS. Un resultado de la protección contra malware para S3 indica que el objeto cargado que inició el análisis de malware contiene un archivo potencialmente malicioso.

Para que Amazon GuardDuty genere un resultado en la Cuenta de AWS, habilite tanto GuardDuty como la protección contra malware para S3. La práctica recomendada es primero habilitar GuardDuty y luego la protección contra malware para S3. Si este orden varía en su caso, asegúrese de habilitar GuardDuty antes de que un objeto de S3 se cargue en el bucket protegido.

Note

GuardDuty no puede generar un resultado para un objeto de S3 que fue analizado antes de habilitar GuardDuty. Para analizar un objeto de S3 existente, puede cargarlo de nuevo.

Object:S3/MaliciousFile

Se ha detectado un archivo malicioso en un objeto de S3 analizado.

Gravedad predeterminada: alta

- Característica: protección contra malware para S3

Este resultado indica que un análisis de malware ha detectado que el objeto de S3 enumerado es malicioso. Para obtener más información, consulte la sección Amenazas detectadas en el panel de detalles del resultado.

Recomendaciones de corrección:

Si este resultado fue inesperado, el objeto de S3 es potencialmente malicioso. Para obtener información sobre los pasos de corrección recomendados, consulte [Corregir un objeto de S3 potencialmente malicioso](#).

Tipos de resultados de la protección de RDS en GuardDuty

La protección de RDS en GuardDuty detecta un comportamiento de inicio de sesión anómalo en la instancia de la base de datos. Los siguientes resultados son específicos de [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) y tendrán un Tipo de recurso de RDSDBInstance o RDSLimitlessDB. La gravedad y los detalles de los resultados variarán en función del tipo de resultado.

Temas

- [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 usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta de forma anómala.

Gravedad predeterminada: variable

 Note

Según el comportamiento anómalo asociado a este resultado, la gravedad predeterminada puede ser baja, media y alta.

- **Baja:** si el nombre de usuario asociado a este resultado inició sesión desde una dirección IP asociada a una red privada.
- **Media:** si el nombre de usuario asociado a este resultado inició sesión desde una dirección IP pública.
- **Alto:** si hay un patrón constante de intentos de inicio de sesión fallidos desde direcciones IP públicas, lo que indica que las políticas de acceso son demasiado permisivas.

- **Característica:** supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que se ha observado un inicio de sesión correcto y anómalo en una base de datos de RDS de su entorno de AWS. Esto puede indicar que un usuario anteriormente invisible inició sesión en una base de datos de RDS por primera vez. Un escenario común es el de un usuario interno que inicia sesión en una base de datos a la que acceden mediante programación las aplicaciones y no los usuarios individuales.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado este inicio de sesión correcto como anómalo. El modelo de ML evalúa todos los eventos de inicio de sesión a la base de datos en su [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML rastrea varios factores de la actividad de inicio de sesión en RDS, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y los detalles específicos de la conexión a la base de datos que se utilizaron. Para obtener información sobre los eventos de inicio de sesión que son potencialmente inusuales, consulte [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, se recomienda cambiar la contraseña del usuario de la base de datos asociada y revisar los registros de auditoría disponibles para ver si hay actividad hechas por el usuario anómalo. Los resultados de gravedad media y alta

pueden indicar que existe una política de acceso demasiado permisiva a la base de datos y que las credenciales de los usuarios pueden haber quedado expuestas o haberse visto afectadas. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Se observaron uno o más intentos de inicio de sesión fallidos inusuales en una base de datos de RDS de su cuenta.

Gravedad predeterminada: baja

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que se observaron uno o más inicios de sesión fallidos anómalos en una base de datos de RDS de su entorno de AWS. Un intento de inicio de sesión fallido desde direcciones IP públicas puede indicar que la base de datos de RDS de su cuenta ha sido objeto de un intento de ataque de fuerza bruta por parte de un actor potencialmente malicioso.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado estos inicios de sesión fallidos como anómalo. El modelo de ML evalúa todos los eventos de inicio de sesión a la base de datos en su [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML rastrea varios factores de la actividad de inicio de sesión en RDS, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y los detalles específicos de la conexión a la base de datos que se utilizaron. Para obtener información sobre la actividad de inicio de sesión en RDS que puede ser inusual, consulte [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que la base de datos está expuesta públicamente o que existe una política de acceso demasiado permisiva a la base de datos. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más

información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP pública de forma anómala tras un patrón constante de intentos de inicio de sesión fallidos e inusuales.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que se ha observado un inicio de sesión anómalo, lo que indica el uso de una fuerza bruta exitosa, en una base de datos de RDS de su entorno de AWS. Antes de iniciar sesión correctamente de forma anómala, se observaba un patrón constante de intentos de inicio de sesión fallidos inusuales. Esto indica que es posible que el usuario y la contraseña asociados a la base de datos de RDS de su cuenta se hayan visto afectados y que un actor potencialmente malicioso haya accedido a la base de datos de RDS.

El modelo de machine learning (ML) de detección de anomalías de GuardDuty ha identificado este inicio de sesión de fuerza bruta como anómalo. El modelo de ML evalúa todos los eventos de inicio de sesión a la base de datos en su [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML rastrea varios factores de la actividad de inicio de sesión en RDS, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y los detalles específicos de la conexión a la base de datos que se utilizaron. Para obtener información sobre la actividad de inicio de sesión en RDS que puede ser inusual, consulte [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

Recomendaciones de corrección:

Esta actividad indica que las credenciales de la base de datos pueden estar expuestas o que se hayan visto afectadas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad que ha llevado a cabo el usuario potencialmente afectado. Un patrón constante de intentos de inicio de sesión fallidos inusuales es indicador de una política de acceso demasiado permisiva a la base de datos o que

la base de datos también puede haber estado expuesta al público. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que se ha producido una actividad de inicio de sesión correcta en RDS desde una dirección IP asociada a una actividad maliciosa conocida en su entorno de AWS. Esto indica que es posible que el usuario y la contraseña asociados a la base de datos de RDS de su cuenta se hayan visto afectados y que un actor potencialmente malicioso haya accedido a la base de datos de RDS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que las credenciales del usuario pueden estar expuestas o haberse visto afectadas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad que ha llevado a cabo el usuario afectado. Esta actividad también puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Una dirección IP asociada a una actividad maliciosa conocida intentó iniciar sesión sin éxito en una base de datos de RDS de su cuenta.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que una dirección IP asociada a una actividad maliciosa conocida intentó iniciar sesión en una base de datos de RDS de su entorno de AWS, pero no proporcionó el nombre de usuario o la contraseña correctos. Esto indica que un actor potencialmente malicioso podría estar intentando afectar a la base de datos de RDS de su cuenta.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

Discovery:RDS/MaliciousIPCaller

Una dirección IP asociada a una actividad maliciosa conocida ha sondeado una base de datos de RDS de su cuenta; no se ha llevado a cabo ningún intento de autenticación.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que una dirección IP asociada a una actividad maliciosa conocida ha sondeado una base de datos de RDS de su entorno de AWS, aunque no se ha llevado a cabo ningún intento de inicio de sesión. Esto puede indicar que un actor potencialmente malicioso está intentando buscar una infraestructura de acceso público.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del

grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que un usuario ha iniciado sesión correctamente en una base de datos de RDS de su entorno de AWS desde una dirección IP de nodo de salida de Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de RDS de su cuenta con la intención de ocultar la verdadera identidad del usuario anónimo.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que las credenciales del usuario pueden estar expuestas o haberse visto afectadas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad que ha llevado a cabo el usuario afectado. Esta actividad también puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

CredentialAccess:RDS/TorIPCaller.FailedLogin

Una dirección IP de Tor intentó iniciar sesión sin éxito en una base de datos de RDS de su cuenta.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que una dirección IP de nodo de salida de Tor intentó iniciar sesión en una base de datos de RDS de su entorno de AWS, pero no proporcionó el nombre de usuario o la contraseña correctos. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de RDS de su cuenta con la intención de ocultar la verdadera identidad del usuario anónimo.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

Discovery:RDS/TorIPCaller

Una dirección IP de nodo de salida de Tor ha sondeado una base de datos de RDS de su cuenta, pero no se ha llevado a cabo ningún intento de autenticación.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado indica que una dirección IP de nodo de salida de Tor ha sondeado una base de datos de RDS de su entorno de AWS, aunque no se ha llevado a cabo ningún intento de inicio de sesión. Esto puede indicar que un actor potencialmente malicioso está intentando buscar una infraestructura de acceso público. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de RDS de su cuenta con la intención de ocultar la verdadera identidad del actor potencialmente malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

Tipos de resultados de la protección de Lambda

En esta sección, se describen los tipos de resultados que son específicos de sus recursos de AWS Lambda cuyo `resourceType` se muestra en una lista como Lambda. Para todos los resultados de Lambda, se recomienda examinar el recurso en cuestión y determinar si se comporta de la manera esperada. Si la actividad está autorizada, puede utilizar [reglas de supresión](#) o [listas de IP confiables y de amenazas](#) para evitar las notificaciones de falsos positivos de ese recurso.

Si la actividad es inesperada, la práctica recomendada de seguridad consiste en suponer que Lambda posiblemente se ha visto afectado y seguir las recomendaciones de corrección.

Temas

- [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 función de Lambda está consultando una dirección IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que hay una función de Lambda que aparece en la lista dentro del entorno de AWS que está consultando una dirección IP asociada con un servidor de comando y control (C&C) conocido. La función de Lambda asociada al resultado generado se ha visto potencialmente afectada. Los servidores C&C son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet, que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas, que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función del propósito y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar una denegación de servicio distribuida.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

CryptoCurrency:Lambda/BitcoinTool.B

Una función de Lambda consulta una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que la función de Lambda que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de las funciones de Lambda para reutilizarlas maliciosamente para la extracción no autorizada de criptomonedas.

Recomendaciones de corrección:

Si utiliza esta función de Lambda para extraer o administrar criptomonedas, o esta función está involucrada de otra manera en la actividad de cadena de bloques, esto podría representar una actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de

dos criterios de filtro. El primer criterio debe utilizar el atributo de tipo de resultado con un valor `CryptoCurrency:Lambda/BitcoinTool.B`. El segundo criterio de filtro debe ser el nombre de la función de Lambda de la función implicada en la actividad de la cadena de bloques. Para obtener información sobre la creación de reglas de supresión, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

Trojan:Lambda/BlackholeTraffic

Una función de Lambda está intentando comunicarse con una dirección IP de un host remoto que es una dirección IP de agujero negro conocida.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que una función de Lambda incluida en la lista de su entorno de AWS está intentando comunicarse con una dirección IP de un agujero negro (u oculta). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host. La función de Lambda que aparece en la lista se ha visto potencialmente afectada.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

Trojan:Lambda/DropPoint

Una función de Lambda está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que una función de Lambda dentro de su entorno de AWS está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Una función de Lambda lleva a cabo conexiones a una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que una función de Lambda del entorno de AWS está comunicándose con una dirección IP incluida en una lista de amenazas que se ha cargado. En GuardDuty, una [lista de amenazas](#) está formada por direcciones IP maliciosas conocidas. GuardDuty genera resultados basados en las listas de amenazas cargadas. Puede ver los detalles de la lista de amenazas en los detalles de resultado de la consola de GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

UnauthorizedAccess:Lambda/TorClient

Una función de Lambda está llevando a cabo conexiones con un nodo Authority o Guard de Tor.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que una función de Lambda del entorno de AWS está llevando a cabo conexiones con un nodo Authority o Guard de Tor. Tor es un software que permite la comunicación anónima. Los nodos Authority y Guard de Tor actúan como puertas de enlace iniciales a una red de Tor. Este tráfico puede indicar que esta función de Lambda se ha visto potencialmente afectada. Ahora actúa como cliente en una red de Tor.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

UnauthorizedAccess:Lambda/TorRelay

Una función de Lambda está estableciendo conexiones a una red de Tor como relé de Tor.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este resultado le informa de que una función de Lambda del entorno de AWS está llevando a cabo conexiones con una red de Tor de una forma que sugiere que actúa como un relé de Tor. Tor es un software que permite la comunicación anónima. Tor habilita la comunicación anónima al reenviar el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

Tipos de resultados retirados

Un resultado es una notificación que contiene detalles sobre un problema potencial de seguridad detectado por GuardDuty. Para obtener más información acerca de cambios importantes en los tipos de resultado de GuardDuty, incluidos los retirados o añadidos recientemente, consulte [Historial de documentación de Amazon GuardDuty](#).

Se han retirado los siguientes tipos de resultados y GuardDuty ya no los genera.

 Important

No se pueden reactivar los tipos de resultados retirados de GuardDuty.

Temas

- [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

Una entidad de IAM ha invocado una API de S3 de forma sospechosa.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

- Origen de datos: eventos de datos de CloudTrail para S3

Este resultado le informa de que una entidad de IAM en su entorno de AWS está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a la fase de exfiltración de un ataque, en la que un atacante intenta recopilar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Impact:S3/PermissionsModification.Unusual

Una entidad de IAM ha invocado una API para modificar los permisos en uno o más recursos de S3.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le informa de que una entidad de IAM está haciendo llamadas a la API diseñadas para modificar los permisos en uno o más buckets u objetos de su entorno de AWS. Es posible que un atacante lleve a cabo esta acción para permitir que la información se comparta fuera de la cuenta. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Impact:S3/ObjectDelete.Unusual

Una entidad de IAM ha invocado una API que se utiliza para eliminar datos en un bucket de S3.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le informa de que una entidad de IAM específica de su entorno de AWS está haciendo llamadas a la API diseñadas para eliminar los datos del bucket de S3 de la lista mediante la eliminación del propio bucket. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Discovery:S3/BucketEnumeration.Unusual

Una entidad de IAM ha invocado una API de S3 que se utiliza para detectar los buckets de S3 dentro de la red.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le informa de que una entidad de IAM ha invocado una API de S3 para detectar los buckets de S3 en su entorno, como, por ejemplo, `ListBuckets`. Este tipo de actividad está asociada a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Persistence:IAMUser/NetworkPermissions

Una entidad de IAM ha invocado una API que se suele utilizar para cambiar los permisos de acceso a la red de los grupos de seguridad, las rutas y las ACL de su cuenta de AWS.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le indica que una entidad principal específica (Usuario raíz de la cuenta de AWS, rol de IAM o usuario) del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena cuando los ajustes de configuración de la red se modifican en circunstancias sospechosas, como cuando una entidad principal invoca la API de `CreateSecurityGroup` sin antecedentes de haberlo hecho. A menudo, los atacantes intentan cambiar los grupos de seguridad para permitir que cierta cantidad de tráfico entre en varios puertos a fin de mejorar su capacidad para obtener acceso a una instancia de EC2.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Persistence:IAMUser/ResourcePermissions

Una entidad principal ha invocado una API que suele utilizarse para cambiar las políticas de acceso de seguridad de varios recursos de su Cuenta de AWS.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le indica que una entidad principal específica (Usuario raíz de la cuenta de AWS, rol de IAM o usuario) del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida. Esta entidad principal nunca antes había invocado esta API.

Este resultado se activa cuando se detecta un cambio en las políticas o los permisos asociados a recursos de AWS; por ejemplo, cuando una entidad principal de su entorno de AWS invoca la API de `PutBucketPolicy` sin tener un historial previo de haberlo hecho. Algunos servicios, como Amazon S3, tienen permisos asociados a recursos que conceden a una o más entidades principales acceso a dicho recurso. Con las credenciales robadas, los atacantes pueden cambiar las políticas asociadas a un recurso para obtener acceso a dicho recurso.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Persistence:IAMUser/UserPermissions

Una entidad principal ha invocado una API que suele utilizarse para agregar, modificar o eliminar políticas, grupos o usuarios de IAM de una cuenta de AWS.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le indica que una entidad principal específica (Usuario raíz de la cuenta de AWS, rol de IAM o usuario) del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena debido a cambios sospechosos en los permisos relacionados con los usuarios de su entorno de AWS: por ejemplo, cuando una entidad principal de su entorno de AWS invoca la API de `AttachUserPolicy` sin tener antecedentes de hacerlo. Los atacantes pueden utilizar credenciales robadas para crear nuevos usuarios, agregar políticas de acceso a los usuarios

existentes o crear claves de acceso para maximizar su acceso a una cuenta, incluso si su punto de acceso original está cerrado. Por ejemplo, el propietario de la cuenta podría darse cuenta del robo de una contraseña o un usuario de IAM en concreto y eliminarlos de la cuenta. Sin embargo, es posible que no elimine otros usuarios que haya creado una entidad principal administradora creada de forma fraudulenta, lo que dejaría su cuenta de AWS accesible al atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

PrivilegeEscalation:IAMUser/AdministrativePermissions

Una entidad principal ha intentado asignarse una política excesivamente permisiva.

Gravedad predeterminada: baja*

Note

La gravedad de este resultado es baja si no se consigue completar el intento de escalado de privilegios o media si el intento se lleva a cabo con éxito.

Este resultado le informa de que una entidad de IAM específica del entorno de AWS está mostrando un comportamiento que puede indicar un ataque de derivación de privilegios. Este resultado se desencadena cuando un rol o un usuario de IAM intentan asignarse una política excesivamente permisiva. Si el usuario o el rol en cuestión no debe tener privilegios administrativos, puede que las credenciales del usuario estén en riesgo o que los permisos del rol no se hayan configurado correctamente.

Los atacantes utilizarán credenciales robadas para crear nuevos usuarios, agregar políticas de acceso a los usuarios existentes o crear claves de acceso para maximizar su acceso a una cuenta incluso si su punto de acceso original está cerrado. Por ejemplo, el propietario de la cuenta podría percatarse de que le han robado una credencial de inicio de sesión de un usuario de IAM específico y eliminarla de la cuenta. Sin embargo, es posible que no elimine otros usuarios creados por la entidad principal de administración creada de forma fraudulenta, lo que aún dejaría su cuenta de AWS accesible para el atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Recon:IAMUser/NetworkPermissions

Una entidad principal ha invocado una API que suele usarse para cambiar los permisos de acceso de red de los grupos de seguridad, las rutas y las ACL de la cuentas de AWS.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le indica que una entidad principal específica (Usuario raíz de la cuenta de AWS, rol de IAM o usuario) del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena cuando se sondean los permisos de acceso a recursos de su cuenta de AWS en circunstancias sospechosas. Por ejemplo, si una entidad principal invoca la API `DescribeInstances` cuando no tiene antecedentes de haberlo hecho. Un atacante podría utilizar credenciales robadas para llevar a cabo este tipo de reconocimiento de sus recursos de AWS y encontrar de esta manera más credenciales valiosas o determinar cuáles son las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Recon:IAMUser/ResourcePermissions

Una entidad principal ha invocado una API que suele utilizarse para cambiar las políticas de acceso de seguridad de varios recursos de una cuenta de AWS.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado le indica que una entidad principal específica (Usuario raíz de la cuenta de AWS, rol de IAM o usuario) del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena cuando se sondean los permisos de acceso a recursos de su cuenta de AWS en circunstancias sospechosas. Por ejemplo, si una entidad principal invoca la API `DescribeInstances` cuando no tiene antecedentes de haberlo hecho. Un atacante podría utilizar credenciales robadas para llevar a cabo este tipo de reconocimiento de sus recursos de AWS y encontrar de esta manera más credenciales valiosas o determinar cuáles son las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Recon:IAMUser/UserPermissions

Una entidad principal ha invocado una API que suele utilizarse para agregar, modificar o eliminar políticas, grupos o usuarios de IAM de una cuenta de AWS.

Gravedad predeterminada: media*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado se desencadena cuando se sondean los permisos de usuario de su entorno de AWS en circunstancias sospechosas. Por ejemplo, si una entidad principal (Usuario raíz de la cuenta de AWS, rol de IAM o usuario de IAM) invoca la API `ListInstanceProfilesForRole` cuando no tiene antecedentes de haberlo hecho. Un atacante podría utilizar credenciales robadas para llevar a cabo este tipo de reconocimiento de sus recursos de AWS y encontrar de esta manera más credenciales valiosas o determinar cuáles son las capacidades de las credenciales que ya tiene.

Este resultado le indica que una entidad principal específica del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida. Esta entidad principal no tiene historial previo de invocación de esta API de esta manera.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

ResourceConsumption:IAMUser/ComputeResources

Una entidad principal ha invocado una API que suele utilizarse para lanzar recursos de computación como instancias EC2.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado se desencadena cuando se lanzan instancias de EC2, que aparecen en la cuenta mostrada en la lista, dentro de su entorno de AWS en circunstancias sospechosas. Este resultado le indica que una entidad principal específica del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida; por ejemplo, si una entidad principal (Usuario raíz de la cuenta de AWS, rol de IAM o usuario de IAM) invoca la API `RunInstances` sin tener antecedentes de haberlo hecho. Esto podría ser señal de que un atacante está utilizando credenciales robadas

para robar tiempo de computación (posiblemente para minería de criptomoneda o violación de contraseñas). También puede indicar que un atacante está utilizando una instancia de EC2 de su entorno de AWS y sus credenciales para mantener el acceso a su cuenta.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Stealth:IAMUser/LoggingConfigurationModified

Una entidad principal ha invocado una API que suele utilizarse para parar el registro en CloudTrail, borrar los registros existentes y eliminar de cualquier otra forma los rastros de la actividad de una cuenta de AWS.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado se desencadena cuando se modifica la configuración de registro de la cuenta de AWS, que aparece en la lista, en circunstancias sospechosas. Este resultado le informa de que una entidad principal específica del entorno de AWS está mostrando un comportamiento diferente de la referencia establecida; por ejemplo, si una entidad principal (Usuario raíz de la cuenta de AWS, rol de IAM o usuario de IAM) invoca la API `StopLogging` sin tener antecedentes de haberlo hecho. Esto puede ser señal de que un atacante está intentando cubrir sus huellas eliminando cualquier rastro de su actividad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:IAMUser/ConsoleLogin

Se ha observado que una entidad principal de su cuenta de AWS ha iniciado sesión de forma inusual en la consola.

Gravedad predeterminada: media*

Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia, la gravedad del resultado será alta.

Este resultado se desencadena cuando se detecta un inicio de sesión en la consola en circunstancias sospechosas. Por ejemplo, si una entidad principal sin antecedentes de haberlo hecho, ha invocado la API de ConsoleLogin desde un cliente nunca antes usado o una ubicación inusual. Esto podría indicar que se están utilizando credenciales robadas para obtener acceso a su cuenta de AWS o que un usuario válido está obteniendo acceso a la cuenta de forma no válida o menos segura (por ejemplo, no accede mediante una VPN aprobada).

Este resultado le informa de que una entidad principal específica del entorno de AWS está mostrando un comportamiento diferente a la referencia establecida. Esta entidad principal nunca antes había iniciado sesión con esta aplicación cliente desde esta ubicación específica.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

UnauthorizedAccess:EC2/TorIPCaller

La instancia EC2 recibe conexiones entrantes de un nodo de salida Tor.

Gravedad predeterminada: media

Este resultado le informa de que una instancia de EC2 del entorno de AWS está recibiendo conexiones entrantes de un nodo de salida de Tor. Tor es un software que permite la comunicación

anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Este resultado puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Backdoor:EC2/XORDDOS

Una instancia de EC2 está intentando comunicarse con una dirección IP asociada con malware XOR DDoS.

Gravedad predeterminada: alta

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que intenta comunicarse con una dirección IP relacionada con malware XOR DDoS. Esta instancia de EC2 podría estar comprometida. XOR DDoS es malware troyano que secuestra sistemas Linux. En un intento de obtener acceso al sistema, lanza un ataque de fuerza bruta para descubrir la contraseña a los servicios de Secure Shell (SSH) en Linux. Después de haber adquirido las credenciales de SSH y haber llevado a cabo correctamente el inicio de sesión, utiliza privilegios de usuario raíz para ejecutar un script que descarga e instala XOR DDoS. A continuación, este malware se utiliza como parte de un botnet para lanzar ataques de denegación de servicio distribuida (DDoS) contra otros destinos.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Behavior:IAMUser/InstanceLaunchUnusual

Un usuario ha lanzado una instancia de EC2 de un tipo inusual.

Gravedad predeterminada: alta

Este resultado le informa de que un usuario específico del entorno de AWS está mostrando un comportamiento distinto de la referencia establecida. Este usuario no tiene historial previo de lanzamientos de una instancia de EC2 de este tipo. Sus credenciales de inicio de sesión podrían haberse visto afectadas.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

CryptoCurrency:EC2/BitcoinTool.A

La instancia EC2 se está comunicando con grupos de minería de Bitcoin.

Gravedad predeterminada: alta

Este resultado le informa de que una instancia de EC2 del entorno de AWS se está comunicando con grupos de extracción de Bitcoin. En el campo de la minería de criptomonedas, un grupo de minería es la agrupación de recursos de mineros que comparten potencia de procesamiento a través de una red para dividir la compensación en función de la cantidad de trabajo con la que han contribuido para resolver un bloque. A menos que utilice esta instancia de EC2 para la minería de Bitcoin, dicha instancia podría estar comprometida.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

UnauthorizedAccess:IAMUser/UnusualASNCaller

Se ha invocado una API desde una dirección IP de una red inusual.

Gravedad predeterminada: alta

Este resultado le informa que se ha invocado cierta actividad desde una dirección IP de una red inusual. Esta red no se ha observado nunca en todo el historial de uso de AWS del usuario descrito. Esta actividad puede incluir un inicio de sesión en la consola, un intento de lanzar una instancia de EC2, la creación de un nuevo usuario de IAM, la modificación de sus privilegios de AWS, etc. Esto puede significar un acceso no autorizado a los recursos de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).

Tipos de resultados de GuardDuty por recursos potencialmente impactados

Las páginas siguientes se clasifican según el tipo de recurso potencialmente impactado asociado a un resultado de GuardDuty:

- [Tipos de resultados de EC2](#)
- [Tipos de resultados de IAM](#)
- [Tipos de resultados de secuencias de ataque](#)
- [Tipos de resultados de la S3 Protection](#)
- [Tipos de resultados de la protección de EKS](#)
- [Tipos de resultados de la supervisión en tiempo de ejecución](#)
- [Tipos de resultados de la protección contra malware para EC2](#)
- [Tipo de resultado de la protección contra malware para S3](#)
- [Tipos de resultados de la protección de RDS](#)
- [Tipos de resultados de la protección de Lambda](#)

Tipos de resultados activos de GuardDuty

En la siguiente tabla, se muestran todos los tipos de resultados activos ordenados por el origen de datos o la característica fundamental, según corresponda. En la siguiente tabla, algunos de los resultados tienen los valores de la columna Gravedad de resultados marcados con un asterisco (*) o un signo más (+):

* Estos tipos de resultados tienen una gravedad variable. Un resultado de un tipo concreto puede tener una gravedad diferente según el contexto específico de dicho resultado. Para obtener más información sobre un tipo de resultado, consulte su descripción detallada.

⁺ Los resultados de EC2 que utilizan registros de flujo de VPC como origen de datos no admiten el tráfico IPv6.

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:S3/AnomalousBehavior	Amazon S3	Eventos de datos de CloudTrail para S3	Bajo
Discovery:S3/MaliciousIPCaller	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
Discovery:S3/TorIPCaller	Amazon S3	Eventos de datos de CloudTrail para S3	Medio
Exfiltration:S3/AnomalousBehavior	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
Exfiltration:S3/MaliciousIPCaller	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
Impact:EC2/MaliciousDomainRequest.Custom	Amazon EC2	Registros de DNS	Medio
Impact:S3/AnomalousBehavior.Delete	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
Impact:S3/AnomalousBehavior.Permission	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
Impact:S3/AnomalousBehavior.Write	Amazon S3	Eventos de datos de CloudTrail para S3	Medio
Impact:S3/MaliciousIPCaller	Amazon S3	Eventos de datos de CloudTrail para S3	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
PenTest:S3/KaliLinux	Amazon S3	Eventos de datos de CloudTrail para S3	Medio
PenTest:S3/ParrotLinux	Amazon S3	Eventos de datos de CloudTrail para S3	Medio
PenTest:S3/PentoolLinux	Amazon S3	Eventos de datos de CloudTrail para S3	Medio
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	Eventos de datos de CloudTrail para S3	Alto
CredentialAccess:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Medio
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Medio
Discovery:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Bajo
Exfiltration:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Alto
Impact:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
InitialAccess:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Medio
PenTest:IAMUser/KaliLinux	IAM	Eventos de administración de CloudTrail	Medio
PenTest:IAMUser/ParrrotLinux	IAM	Eventos de administración de CloudTrail	Medio
PenTest:IAMUser/PentooLinux	IAM	Eventos de administración de CloudTrail	Medio
Persistence:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Medio
Stealth:IAMUser/PasswordPolicyChange	IAM	Eventos de administración de CloudTrail	Bajo*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	Eventos de administración de CloudTrail	Alta*
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	Eventos de administración de CloudTrail	Bajo
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	Eventos de administración de CloudTrail	Alto
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	Eventos de administración de CloudTrail	Bajo

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Policy:S3/BucketPublicAccessGranted	Amazon S3	Eventos de administración de CloudTrail	Alto
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	Eventos de administración de CloudTrail	Medio
Recon:IAMUser/MaliciousIPCaller	IAM	Eventos de administración de CloudTrail	Medio
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	Eventos de administración de CloudTrail	Medio
Recon:IAMUser/TorIPCaller	IAM	Eventos de administración de CloudTrail	Medio
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	Eventos de administración de CloudTrail	Bajo
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	Eventos de administración de CloudTrail	Bajo
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	Eventos de administración de CloudTrail	Medio
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	Eventos de administración de CloudTrail	Medio
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	Eventos de administración de CloudTrail	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	Eventos de administración de CloudTrail	Medio
Policy:IAMUser/RootCredentialUsage	IAM	Eventos de administración de CloudTrail o eventos de datos de CloudTrail para S3	Bajo
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	Eventos de administración de CloudTrail o eventos de datos de CloudTrail para S3	Bajo
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	Eventos de administración de CloudTrail o eventos de datos de CloudTrail para S3	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
AttackSequence:EKS/CompromisedCluster	Recursos involucrados en la secuencia de ataque	• Eventos de registro de auditoría de EKS • Runtime Monitoring de Amazon EKS • Detección de malware de Amazon EKS para Amazon EC2 • Eventos de datos de AWS CloudTrail para S3 • Eventos de administración de AWS CloudTrail • Logs de flujo de VPC • Registros de consultas de DNS de Route53 Resolver	Critico
AttackSequence:IAM/CompromisedCredentials	Recursos involucrados en la secuencia de ataque	Eventos de administración de CloudTrail	Critico
AttackSequence:S3/CompromisedData	Recursos involucrados en la secuencia de ataque	Eventos de administración de CloudTrail y eventos de datos de CloudTrail para S3	Critico
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Registros de DNS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Registros de DNS	Alto
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Registros de DNS	Medio
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Registros de DNS	Alto
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Registros de DNS	Alto
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Registros de DNS	Bajo
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Registros de DNS	Medio
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Registros de DNS	Alto
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Registros de DNS	Alto
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Registros de DNS	Alto
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Registros de DNS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Trojan:EC2/DropPoint!DNS	Amazon EC2	Registros de DNS	Medio
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Registros de DNS	Alto
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Registros de DNS	Alto
Execution:Container/MaliciousFile	Contenedor	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:Container/SuspiciousFile	Contenedor	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:EC2/MaliciousFile	Amazon EC2	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:EC2/SuspiciousFile	Amazon EC2	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:ECS/MaliciousFile	ECS	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:ECS/SuspiciousFile	ECS	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:Kubernetes/MaliciousFile	Kubernetes	Protección contra malware de EBS	Varía en función de la amenaza detectada
Execution:Kubernetes/SuspiciousFile	Kubernetes	Protección contra malware de EBS	Varía en función de la amenaza detectada

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Registros de auditoría de EKS	Medio
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de EKS	Alto
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de EKS	Alto
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de EKS	Alto
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de EKS	Alto
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de EKS	Alto
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de EKS	Alto
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de EKS	Alto
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de EKS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Registros de auditoría de EKS	Bajo
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de EKS	Medio
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de EKS	Medio
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de EKS	Medio
Discovery:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de EKS	Medio
Execution:Kubernetes/ExecInKubernetesPod	Kubernetes	Registros de auditoría de EKS	Medio
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Registros de auditoría de EKS	Medio
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Registros de auditoría de EKS	Bajo
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de EKS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de EKS	Alto
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de EKS	Alto
Impact:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de EKS	Alto
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Registros de auditoría de EKS	Medio
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de EKS	Medio
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de EKS	Medio
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de EKS	Alto
Persistence:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de EKS	Medio
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Registros de auditoría de EKS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Registros de auditoría de EKS	Alto
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Registros de auditoría de EKS	Medio
Policy:Kubernetes/ExposedDashboard	Kubernetes	Registros de auditoría de EKS	Medio
PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleBindingCreated	Kubernetes	Registros de auditoría de EKS	Medio*
PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleCreated	Kubernetes	Registros de auditoría de EKS	Bajo
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Registros de auditoría de EKS	Alto
PrivilegeEscalation:Kubernetes/AnonymousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Registros de auditoría de EKS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Registros de auditoría de EKS	Medio
Backdoor:Lambda/C&CActivity.B	Lambda	Supervisión de la actividad de red de Lambda	Alto
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Supervisión de la actividad de red de Lambda	Alto
Trojan:Lambda/BlackholeTraffic	Lambda	Supervisión de la actividad de red de Lambda	Medio
Trojan:Lambda/DropPoint	Lambda	Supervisión de la actividad de red de Lambda	Medio
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Supervisión de la actividad de red de Lambda	Medio
UnauthorizedAccess:Lambda/TorClient	Lambda	Supervisión de la actividad de red de Lambda	Alto
UnauthorizedAccess:Lambda/TorRelay	Lambda	Supervisión de la actividad de red de Lambda	Alto
Object:S3/MaliciousFile	S3Object	Protección contra malware para S3	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Bajo
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Alto
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Variable*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Medio
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Alto
CredentialAccess:RDS/TorIPCaller.FailedLogin	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Medio
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:RDS/MaliciousIPCaller	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Medio
Discovery:RDS/TorIPCaller	Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles	Supervisión de la actividad de inicio de sesión de RDS	Medio
Backdoor:Runtime/C&CActivity.B	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Backdoor:Runtime/C&CActivity.B!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
CryptoCurrency:Runtime/BitcoinTool.B	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
DefenseEvasion:Runtime/FilelessExecution	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
DefenseEvasion:Runtime/KernelModuleLoaded	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
DefenseEvasion:Runtime/ProcessInjection.Proc	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
DefenseEvasion:Runtime/PtraceAntiDebugging	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Bajo
DefenseEvasion:Runtime/SuspiciousCommand	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Discovery:Runtime/SuspiciousCommand	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Bajo
Execution:Runtime/MaliciousFileExecuted	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Execution:Runtime/NewBinaryExecuted	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Execution:Runtime/NewLibraryLoaded	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Execution:Runtime/SuspiciousCommand	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Variable
Execution:Runtime/SuspiciousShellCreated	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Bajo
Execution:Runtime/SuspiciousTool	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Variable
Execution:Runtime/ReverseShell	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Impact:Runtime/AbusedDomainRequest.Reputation	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Impact:Runtime/BitcoinDomainRequest.Reputation	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Impact:Runtime/CryptoMinerExecuted	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Impact:Runtime/MaliciousDomainRequest.Reputation	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
<u>Impact:Runtime/SuspiciousDomainRequest.Reputation</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Bajo
<u>Persistence:Runtime/SuspiciousCommand</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
<u>PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
<u>PrivilegeEscalation:Runtime/ContainerMountsHostDirectory</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
<u>PrivilegeEscalation:Runtime/DockerSocketAccessed</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
<u>PrivilegeEscalation:Runtime/ElevationToRoot</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
<u>PrivilegeEscalation:Runtime/RuncContainerEscape</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
<u>PrivilegeEscalation:Runtime/SuspiciousCommand</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
<u>PrivilegeEscalation:Runtime/UserfaultfdUsage</u>	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Trojan:Runtime/BlackholeTraffic	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/BlackholeTraffic!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/DropPoint	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/DGA DomainRequest.C!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Trojan:Runtime/DriveBySourceTraffic!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Trojan:Runtime/DropPoint!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/PhishingDomainRequest!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
UnauthorizedAccess:Runtime/TorClient	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
UnauthorizedAccess:Runtime/TorRelay	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alto
Backdoor:EC2/C&CActivity.B	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Backdoor:EC2/DenialOfService.Dns	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Backdoor:EC2/DenialOfService.Tcp	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Backdoor:EC2/DenialOfService.Udp	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Backdoor:EC2/DenialOfService.UnusualProtocol	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Backdoor:EC2/Spambot	Amazon EC2	Logs de flujo de VPC ⁺	Medio
Behavior:EC2/NetworkPortUnusual	Amazon EC2	Logs de flujo de VPC ⁺	Medio
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	Logs de flujo de VPC ⁺	Medio
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	Logs de flujo de VPC ⁺	Alto

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	Logs de flujo de VPC ⁺	Medio
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	Logs de flujo de VPC ⁺	Medio
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	Logs de flujo de VPC ⁺	Medio
Impact:EC2/PortSweep	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Impact:EC2/WinRMBruteForce	Amazon EC2	Logs de flujo de VPC ⁺	Bajo [*]
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	Logs de flujo de VPC ⁺	Alto
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	Logs de flujo de VPC ⁺	Bajo [*]
Recon:EC2/Portscan	Amazon EC2	Logs de flujo de VPC ⁺	Medio
Trojan:EC2/BlackholeTraffic	Amazon EC2	Logs de flujo de VPC ⁺	Medio
Trojan:EC2/DropPoint	Amazon EC2	Logs de flujo de VPC ⁺	Medio
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	Logs de flujo de VPC ⁺	Medio
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	Logs de flujo de VPC ⁺	Bajo [*]

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	Logs de flujo de VPC ⁺	Bajo [*]
UnauthorizedAccess:EC2/TorClient	Amazon EC2	Logs de flujo de VPC ⁺	Alto
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	Logs de flujo de VPC ⁺	Alto

Comprender y generar resultados de Amazon GuardDuty

Un resultado de GuardDuty representa un problema de seguridad potencial detectado en Cuentas de AWS, cargas de trabajo y datos. GuardDuty genera resultados inesperados cuando detecta actividades inesperadas y potencialmente maliciosas en el entorno de AWS.

Puede ver y administrar los resultados de GuardDuty en la página Resultados en la consola de GuardDuty, o mediante la AWS CLI o las operaciones de la API. Para obtener información sobre cómo administrar los resultados de GuardDuty, consulte [Administración de resultados de Amazon GuardDuty](#).

Temas:

[Formato de resultado de GuardDuty](#)

Comprenda el formato de los tipos de resultados de GuardDuty y los diferentes propósitos de amenazas que GuardDuty rastrea.

[Hallazgos de ejemplo](#)

Genere resultados de muestra en la consola de GuardDuty, o mediante el uso de la API o los comandos de la AWS CLI GuardDuty. Los resultados de muestra generados incluyen detalles ficticios que ayudan a comprender los detalles del resultado relacionados con cada resultado de GuardDuty. Estos resultados llevan el prefijo [MUESTRA].

[Pruebe los resultados de GuardDuty en cuentas dedicadas](#)

Puede probar resultados específicos de GuardDuty en el entorno. Ejecute el script `guardduty-tester` en una Cuenta de AWS dedicada que no sea de producción. Para que GuardDuty detecte y simule resultados, implementará ciertos recursos en el entorno. Esta experiencia es diferente de la generación de resultados de muestra.

[Ver los resultados generados en la consola de GuardDuty](#)

Obtenga información para revisar los resultados generados en la consola de GuardDuty.

[Niveles de gravedad de los resultados de GuardDuty](#)

Cada resultado de GuardDuty tiene un nivel de gravedad asociado que refleja el riesgo potencial en el entorno de AWS. En esta sección se explica el significado de cada nivel de gravedad.

[Detalles de los resultados](#)

Obtenga información sobre los detalles asociados a los resultados de GuardDuty que se generan en la cuenta. Este tema incluye los detalles asociados con la detección fundamental de amenazas, Detección Extendida de Amenazas así como los planes de protección dedicados en GuardDuty.

[Agregación de resultados de GuardDuty](#)

Obtenga información sobre cómo GuardDuty gestiona múltiples incidencias del mismo tipo de resultado. Al agregar los mismos tipos de resultados detectados, GuardDuty actualiza el tipo de resultado original con los detalles más recientes.

[Tipos de resultados de GuardDuty](#)

En esta sección se enumeran los tipos de hallazgo de GuardDuty por el [Orígenes de datos fundamentales](#) o [Característica de asignaciones de GuardDuty](#) asociados. Para obtener más información sobre cada tipo de resultado, selecciónelo para obtener más detalles, como su descripción y las posibles medidas para corregirlo.

Formato de resultado de GuardDuty

Cuando GuardDuty detecta un comportamiento inesperado o sospechoso en el entorno de AWS, genera un resultado. Un resultado es una notificación que contiene los detalles sobre un posible problema de seguridad detectado por GuardDuty. [Ver los resultados generados en la consola de GuardDuty](#) incluye información sobre lo que ocurrió, qué recursos de AWS participaron en la actividad sospechosa, cuándo se produjo esta actividad e información relacionada que puede servir para comprender la causa raíz.

Uno de los datos más útiles de los detalles de los resultados es el tipo de resultado. El objetivo del tipo de resultado es proporcionar una descripción concisa pero comprensible del posible problema de seguridad. Por ejemplo, el tipo de resultado Recon:EC2/PortProbeUnprotectedPort de GuardDuty le informa inmediatamente de que en algún lugar del entorno de AWS hay una instancia de EC2 con un puerto sin protección que un posible atacante está sondeando.

GuardDuty utiliza el formato siguiente para nombrar los distintos tipos de resultados que genera:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

Cada parte de este formato representa un aspecto de un tipo de resultado. Estos aspectos tienen las siguientes explicaciones:

- **ThreatPurpose:** describe el objetivo principal de una amenaza, un tipo de ataque o una fase de un posible ataque. Consulte la siguiente sección para obtener una lista completa de los propósitos de las amenazas de GuardDuty.
- **ResourceTypeAffected:** describe el tipo de recurso de AWS que se ha identificado en este resultado como el posible objetivo de un adversario. Actualmente, GuardDuty puede generar resultados para los tipos de recursos que se enumeran en [Tipos de resultados activos de GuardDuty](#).
- **ThreatFamilyName:** describe la amenaza general o la posible actividad maliciosa que GuardDuty está detectando. Por ejemplo, el valor `NetworkPortUnusual` indica que una instancia de EC2 identificada en el resultado de GuardDuty no tiene historial previo de comunicaciones en un determinado puerto remoto que también se identifica en el resultado.
- **DetectionMechanism:** describe el método con el que GuardDuty ha detectado el resultado. Esto se puede utilizar para indicar una variación de un tipo de resultado común o un resultado que GuardDuty utilizó un mecanismo específico para detectar. Por ejemplo, `Backdoor:EC2/DenialOfService.Tcp` indica que la denegación de servicio (DoS) se ha detectado a través de TCP. La variante UDP es `Backdoor:EC2/DenialOfService.Udp`.

Un valor de `.Custom` indica que GuardDuty detectó el resultado según las listas de amenazas personalizadas. Para obtener más información, consulte [Listas de entidades y listas de direcciones IP](#).

Un valor de `.Reputation` indica que GuardDuty detectó el resultado a partir de un modelo de puntuación de reputación de dominios. Para obtener más información, consulte [Cómo AWS realiza un seguimiento de las principales amenazas de seguridad en la nube y ayuda a eliminarlas](#).

- **Artefacto:** describe un recurso específico que es propiedad de una herramienta que se utiliza en la actividad maliciosa. Por ejemplo, DNS en el tipo de resultado [CryptoCurrency:EC2/BitcoinTool.B!DNS](#) indica que una instancia de Amazon EC2 se comunica con un dominio conocido relacionado con Bitcoin.

Note

El artefacto es opcional y es posible que no se encuentre disponible para todos los tipos de resultados de GuardDuty.

Propósitos de amenaza

En GuardDuty, un propósito de amenaza describe el objetivo principal de una amenaza, un tipo de ataque o una fase de un posible ataque. Por ejemplo, algunos propósitos de amenaza, como Backdoor, indican un tipo de ataque. Sin embargo, algunos propósitos de amenaza, como Impact, se alinean con las [tácticas de MITRE ATT&CK](#). Las tácticas de MITRE ATT&CK indican distintas fases del ciclo de ataque del adversario. En la versión actual de GuardDuty, ThreatPurpose puede tener los valores siguientes:

Backdoor

Este valor indica que un adversario ha afectado y alterado un recurso de AWS y que este es capaz de contactar con su propio servidor de comando y control (C&C) con objeto de recibir más instrucciones para llevar a cabo actividades maliciosas.

Comportamiento

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad distintos de la referencia establecida para los recursos de AWS involucrados.

CredentialAccess

Este valor indica que GuardDuty ha detectado patrones de actividad que un adversario puede utilizar para robar credenciales del entorno, como contraseñas, nombres de usuario y claves de acceso. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Cryptocurrency

Este valor indica que GuardDuty ha detectado que un recurso de AWS de su entorno aloja software asociado a criptomonedas (por ejemplo, Bitcoin).

DefenseEvasion

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para evitar ser detectado mientras se infiltra en su entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Discovery

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para ampliar su conocimiento acerca de sus sistemas y redes internas. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Execution

Este valor indica que GuardDuty ha detectado que un adversario puede intentar ejecutar o ya ha ejecutado código malicioso para explorar el entorno de AWS, o robar datos. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Exfiltration

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario puede utilizar al intentar robar datos del entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Impact

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que sugieren que un adversario está intentando manipular, interrumpir o destruir sus sistemas y datos. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

InitialAccess

Este valor generalmente se asocia con la etapa de acceso inicial de un ataque cuando un adversario intenta establecer acceso al entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Pentest

A veces, los propietarios de recursos de AWS o sus representantes autorizados ejecutan intencionadamente pruebas en las aplicaciones de AWS para descubrir vulnerabilidades, como grupos de seguridad abiertos o claves de acceso demasiado permisivas. Estas pruebas de intrusión son un intento de identificar y bloquear los recursos vulnerables antes de que los descubran los adversarios. Sin embargo, algunas de las herramientas que se utilizan para las pruebas de intrusión autorizadas están disponibles de forma gratuita y, por tanto, los usuarios no autorizados o los adversarios pueden utilizarlas para llevar a cabo pruebas de sondeo. Aunque GuardDuty no puede identificar el verdadero propósito de este tipo de actividad, el valor Pentest indica que GuardDuty está detectando dicha actividad, la cual es similar a la generada por las herramientas de pruebas de intrusión conocidas, y que podría indicar un sondeo malicioso de su red.

Persistencia

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para intentar conservar el acceso a sus sistemas incluso si ya no puede utilizar su ruta de acceso inicial. Por ejemplo, esto podría incluir la creación de un nuevo

usuario de IAM después de obtener acceso a través de las credenciales afectadas de un usuario existente. Cuando se eliminan las credenciales del usuario existente, el adversario retendrá el acceso al nuevo usuario que no se haya detectado como parte del evento original. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Política

Este valor indica que la Cuenta de AWS exhibe un comportamiento contrario a las prácticas recomendadas de seguridad. Por ejemplo, la modificación no intencionada de las políticas de permisos asociadas a los recursos o el entorno de AWS, y el uso de cuentas privilegiadas cuyo uso debería ser escaso o nulo.

PrivilegeEscalation

Este valor le informa de que la entidad principal implicada dentro de su entorno de AWS presenta un comportamiento que un adversario podría utilizar para obtener permisos de nivel superior para acceder a su red. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

Recon

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar al realizar un reconocimiento previo del entorno para determinar cómo puede ampliar su acceso o utilizar los recursos. Por ejemplo, esta actividad puede incluir la búsqueda de vulnerabilidades en el entorno de AWS mediante el sondeo de puertos, la realización de llamadas a API, la enumeración de usuarios y la enumeración de tablas de bases de datos, entre otras cosas.

Stealth

Este valor indica que un adversario está intentando ocultar sus acciones de forma activa. Por ejemplo, podrían utilizar un servidor proxy anonimizador, lo que dificultaría enormemente evaluar la verdadera naturaleza de la actividad.

Trojan

Este valor indica que un ataque está utilizando programas troyanos que llevan a cabo actividad maliciosa sigilosamente. En ocasiones, este software tiene el aspecto de un programa legítimo. A veces, los usuarios ejecutan accidentalmente este software. Otras veces, este software puede ejecutarse automáticamente mediante la explotación de una vulnerabilidad.

UnauthorizedAccess

Este valor indica que GuardDuty está detectando actividad sospechosa o un patrón de actividades sospechosas por parte de un individuo no autorizado.

Motor de análisis de detección de malware de GuardDuty

Amazon GuardDuty cuenta con un motor de análisis creado y administrado internamente y un [proveedor externo](#). Ambos utilizan indicadores de peligro (IoC) procedentes de varias fuentes internas que tienen visibilidad sobre diferentes tipos de malware que pueden tener como objetivo AWS. GuardDuty también tiene definiciones de detección basadas en reglas YARA agregadas por nuestros ingenieros de seguridad, así como detecciones basadas en modelos heurísticos y de machine learning (ML). Al escanear objetos de Amazon S3, la protección contra malware de GuardDuty produce resultados consistentes al escanear el mismo objeto varias veces con las mismas definiciones y motores de análisis. La detección basada en firmas no se limita a la coincidencia de bytes, sino que también incluye fragmentos de código potencialmente complejos, lo que permite al escáner analizar el contenido y tomar decisiones.

El motor de análisis de malware no realiza análisis de comportamiento en vivo, en los que la detonación de malware supervisa la muestra mientras se ejecuta en un sistema real. La solución de GuardDuty es principalmente una detección basada en archivos. Para detectar malware sin archivos, GuardDuty ofrece una solución basada en agentes, como [Supervisión en tiempo de ejecución](#) para Amazon EKS, Amazon EC2 y Amazon ECS (incluido AWS Fargate).

Sin restricción en los formatos de archivo que GuardDuty analiza en busca de malware, los motores de análisis que utiliza pueden detectar diferentes tipos de malware, como criptomineros, ransomware y webshells. El motor de análisis de GuardDuty, completamente administrado, actualiza continuamente la lista de firmas de malware cada 15 minutos.

El motor de análisis forma parte del sistema de inteligencia de amenazas de GuardDuty, que utiliza un componente interno de detonación de malware. Esto permite generar nueva inteligencia sobre amenazas mediante la recopilación autónoma de muestras de malware y archivos benignos provenientes de diversos orígenes. El tipo de IoC de hash de archivo del sistema de inteligencia de amenazas se integra además con el motor de análisis de malware para detectar malware basado en hashes de archivos maliciosos conocidos.

Generación de resultados de muestra en GuardDuty

Amazon GuardDuty ayuda a generar resultados de muestra para visualizar y conocer los diversos tipos de resultados que puede generar. Cuando genera resultados de muestra, GuardDuty rellena la lista de resultados actual con una muestra por cada tipo de resultado admitido, incluidos tipos de resultados de secuencia de ataque.

Las muestras generadas son aproximaciones rellenas con valores de marcador de posición. Estas muestras pueden diferir de los resultados reales del entorno, pero son útiles para probar diversas configuraciones de GuardDuty, como filtros o eventos de EventBridge. Para consultar la lista de valores disponibles para los tipos de resultados, consulte la tabla [Tipos de resultados de GuardDuty](#).

Generación de resultados de muestra a través de la consola o la API de GuardDuty

Elija el método de acceso que prefiera para generar resultados de muestra.

Note

La consola GuardDuty le ayuda a generar uno para cada tipo de resultado. Para generar uno o más tipos de resultados específicos, lleve a cabo los pasos de API/CLI asociados.

Console

Use el procedimiento siguiente para generar resultados de muestra. Este proceso genera un resultado de muestra para cada tipo de resultado de GuardDuty.

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Configuración.
3. En la página Settings, en Sample findings, elija Generate sample findings.
4. En el panel de navegación, seleccione Resultados. Los resultados de muestra se muestran en la página Resultados actuales con el prefijo [SAMPLE].

API/CLI

Puede generar un solo resultado de muestra que coincida con cualquiera de los tipos de resultados de GuardDuty a través de la API [CreateSampleFindings](#). Los valores disponibles para los tipos de resultados se muestran en la tabla [Tipos de resultados de GuardDuty](#).

Esto resulta útil para probar las reglas de Eventos de CloudWatch o la automatización basada en resultados. En el siguiente ejemplo, se muestra cómo generar un solo resultado de muestra del tipo `Backdoor:EC2/DenialofService.Tcp` con la AWS CLI.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
--finding-types Backdoor:EC2/DenialOfService.Tcp
```

El título de los resultados de muestra generados mediante estos métodos siempre comienza con [SAMPLE] en la consola. Los resultados de muestra tienen un valor "sample": true en la sección `additionalInfo` de los detalles de los resultados de JSON.

Para comprender los detalles del resultado, como la gravedad del resultado y el recurso potencialmente comprometido, asociados a los resultados generados, consulte [Niveles de gravedad de los resultados de GuardDuty](#) y [Detalles de los resultados](#).

Para generar algunos resultados comunes basados en una actividad simulada en un lugar dedicado y aislado en la Cuenta de AWS dentro del entorno, consulte [Pruebe los resultados de GuardDuty en cuentas dedicadas](#).

Pruebe los resultados de GuardDuty en cuentas dedicadas

Utilice este documento para ejecutar un script de pruebas que genera resultados de GuardDuty respecto a recursos de prueba que se implementarán en la Cuenta de AWS. Siga estos pasos para comprender y familiarizarse con determinados tipos de resultados de GuardDuty, así como para explorar cómo se presentan los detalles de los resultados en recursos reales dentro de la cuenta. Esta experiencia es diferente a la de generar [Hallazgos de ejemplo](#). Para obtener más información sobre cómo probar los resultados de GuardDuty, consulte [Consideraciones](#).

Contenido

- [Consideraciones](#)
- [El script de la herramienta de pruebas de resultados de GuardDuty puede generar](#)
- [Paso 1: Requisitos previos](#)
- [Paso 2: Implementar los recursos de AWS](#)
- [Paso 3: Ejecute los scripts de la herramienta de pruebas](#)
- [Paso 4: Limpiar los recursos de pruebas de AWS](#)

- [Solución de problemas comunes](#)

Consideraciones

Antes de continuar, tenga en cuenta las siguientes consideraciones:

- GuardDuty recomienda implementar la herramienta de pruebas en una Cuenta de AWS dedicada que no sea de producción. Este enfoque garantizará que pueda identificar correctamente los resultados de GuardDuty generados por la herramienta de pruebas. Además, la herramienta de pruebas de GuardDuty implementa una variedad de recursos que podrían requerir permisos de IAM adicionales a los permitidos en otras cuentas. Al utilizar una cuenta dedicada, se garantiza que los permisos se puedan delimitar correctamente con un límite de cuenta claro.
- El script de la herramienta de pruebas genera más de 100 resultados de GuardDuty con diferentes combinaciones de recursos de AWS. Actualmente, esto no incluye todos los [Tipos de resultados de GuardDuty](#). Para obtener una lista de los tipos de resultados que puede generar con este script de la herramienta de pruebas, consulte [El script de la herramienta de pruebas de resultados de GuardDuty puede generar](#).

Nota

Para visualizar los tipos de búsqueda de secuencias de ataque, el script del probador genera solo [AttackSequence:EKS/CompromisedCluster](#) y [AttackSequence:S3/CompromisedData](#). Para visualizar y comprender las [AttackSequence:IAM/CompromisedCredentials](#), puedes generar los [Hallazgos de ejemplo](#) en su cuenta.

- Para que la herramienta de pruebas de GuardDuty funcione según lo previsto, GuardDuty debe estar habilitado en la cuenta en la que se implementan los recursos de la herramienta de pruebas. Según las pruebas que se ejecutarán, la herramienta de pruebas evalúa si los planes de protección GuardDuty apropiados están habilitados o no. Para cualquier plan de protección que no esté habilitado, GuardDuty solicitará permiso para habilitar los planes de protección necesarios el tiempo suficiente para que GuardDuty realice las pruebas que generarán resultados. Posteriormente, GuardDuty desactivará el plan de protección una vez que la prueba haya finalizado.

Habilitar GuardDuty por primera vez

Cuando GuardDuty se habilita en la cuenta dedicada por primera vez en una región específica, la cuenta quedará automáticamente inscrita en una prueba gratuita de 30 días.

GuardDuty ofrece planes de protección opcionales. Al habilitar GuardDuty, ciertos planes de protección también se habilitan y se incluyen en la prueba gratuita de 30 días de GuardDuty. Para obtener más información, consulte [Utilizar la prueba gratuita de 30 días de GuardDuty](#).

GuardDuty ya está habilitado en la cuenta antes de ejecutar el script de la herramienta de pruebas

Cuando GuardDuty ya está habilitado, en función de los parámetros, el script de la herramienta de pruebas verificará el estado de configuración de ciertos planes de protección y otros ajustes a nivel de cuenta que se requieren para generar los resultados.

Al ejecutar este script de la herramienta de pruebas, es posible que ciertos planes de protección se habiliten por primera vez en la cuenta dedicada en una región. Esto iniciará la prueba gratuita de 30 días para ese plan de protección. Para obtener información sobre la prueba gratuita asociada a cada plan de protección, consulte [Utilizar la prueba gratuita de 30 días de GuardDuty](#).

- Mientras se implemente la infraestructura del comprobador de GuardDuty, es posible que reciba ocasionalmente los resultados de [UnauthorizedAccess:EC2/TorClient](#) de la instancia de las pruebas de penetración.

El script de la herramienta de pruebas de resultados de GuardDuty puede generar

Actualmente, el script de la herramienta de pruebas genera los siguientes tipos de resultados relacionados con los registros de auditoría de Amazon EC2, Amazon EKS, Amazon S3, IAM y 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](#)

Paso 1: Requisitos previos

Para preparar el entorno de prueba, necesitará los siguientes elementos:

- Git: instale la herramienta de línea de comandos git en función del sistema operativo que utilice.

Esto se necesita para clonar el [repositorio de amazon-guardduty-tester](#).

- **AWS Command Line Interface:** una herramienta de código abierto que permite interactuar con Servicios de AWS mediante el uso de comandos en el intérprete de la línea de comandos. Para obtener más información, consulte [Introducción a AWS CLI](#) en la Guía del usuario de AWS Command Line Interface.
- **AWS Systems Manager:** para iniciar sesiones del Administrador de sesiones con los nodos administrados mediante AWS CLI, debe instalar el complemento del Administrador de sesiones en la máquina local. Para obtener más información, consulte [Instalar el complemento del Administrador de sesiones para AWS CLI](#) en la Guía del usuario de AWS Systems Manager
- **Administrador de paquetes de nodos (NPM):** instale el NPM para instalar todas las dependencias.
- **Docker:** debe tener Docker instalado. Para obtener instrucciones de instalación, consulte el [sitio web de Docker](#).

Para verificar que Docker ha sido instalado, ejecute el siguiente comando y confirme que hay una salida similar a la siguiente:

```
$ docker --version
Docker version 19.03.1
```

- Suscríbase a la imagen de [Kali Linux](#) en el AWS Marketplace.

Paso 2: Implementar los recursos de AWS

Esta sección proporciona una lista de conceptos clave y los pasos para implementar determinados recursos de AWS en la cuenta dedicada.

Conceptos

En la siguiente lista se ofrecen conceptos clave relacionados con los comandos que sirven para implementar los recursos:

- **AWS Cloud Development Kit (AWS CDK)** – CDK es un marco de desarrollo de software de código abierto para definir la infraestructura en la nube en el código y su aprovisionamiento a través de CloudFormation. CDK admite un par de lenguajes de programación para definir componentes en la nube reutilizables conocidos como constructos. Puedes combinarlos en pilas y aplicaciones. A continuación, puede implementar las aplicaciones CDK en CloudFormation para aprovisionar o actualizar los recursos. Para obtener más información, consulte [¿Qué es AWS CDK?](#) en la Guía para desarrolladores de AWS Cloud Development Kit (AWS CDK).

- **Arranque:** es el proceso para preparar el entorno de AWS para su uso con AWS CDK. Antes de implementar una pila de CDK en un entorno de AWS, primero se debe arrancar el entorno. Este proceso de aprovisionamiento de recursos específicos de AWS en el entorno que AWS CDK utiliza forma parte de los pasos que seguirá en la siguiente sección: [Pasos para implementar recursos de AWS](#).

Para obtener más información sobre cómo funciona el arranque, consulte [Arranque](#) en la Guía del desarrollador de AWS Cloud Development Kit (AWS CDK).

Pasos para implementar recursos de AWS

Siga los siguientes pasos para comenzar a implementar los recursos:

1. Configure la cuenta y la región predeterminadas de la AWS CLI, a menos que las variables de región de la cuenta dedicada se configuren manualmente en el archivo `bin/cdk-gd-tester.ts`. Para obtener más información, consulte [Entornos](#) en la Guía para desarrolladores de AWS Cloud Development Kit (AWS CDK).
2. Ejecute los siguientes comandos para implementar los recursos:

```
git clone https://github.com/aws-labs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

El último comando (`cdk deploy`) crea una pila CloudFormation en su nombre. El nombre de esta pila es `GuardDutyTesterStack`.

Como parte de este script, GuardDuty crea nuevos recursos para generar resultados de GuardDuty en la cuenta. Además, agrega el siguiente par de clave y valor de etiqueta a las instancias de Amazon EC2:

`CreatedBy:GuardDuty Test Script`

Las instancias de Amazon EC2 también incluyen las instancias de EC2 que alojan nodos de EKS y clústeres de ECS.

Tipos de instancias

GuardDuty está diseñado para utilizar tipos de instancias rentables que proporcionan el rendimiento mínimo necesario para llevar a cabo las pruebas satisfactoriamente. Debido a los requisitos de vCPU, el grupo de nodos de Amazon EKS requiere `t3.medium`, y debido al aumento de la capacidad de red requerida para las pruebas de resultados de DenialOfService, el nodo controlador requiere `m6i.large`. Para todas las demás pruebas, GuardDuty usa el tipo de instancia `t3.micro`. Para obtener más información sobre los tipos de instancias, consulte [Tamaños disponibles](#) en la Guía de tipos de instancias de Amazon EC2.

Paso 3: Ejecute los scripts de la herramienta de pruebas

Este es un proceso de dos pasos en el que primero es necesario iniciar una sesión con el controlador de pruebas y luego, ejecutar scripts para generar resultados de GuardDuty con combinaciones específicas de recursos.

Parte A: Iniciar una sesión con el controlador de la prueba

1. Una vez implementados los recursos, guarde el código de la región en una variable de la sesión de terminal actual. Utilice el siguiente comando y sustituya `us-east-1` por el código de la región en la que ha implementado los recursos:

```
$ REGION=us-east-1
```

2. El script de la herramienta de pruebas solo está disponible a través de AWS Systems Manager (SSM). Para iniciar un intérprete de comandos interactivo en la instancia del host de la herramienta de pruebas, consulte el InstanceID del host.
3. Utilice el siguiente comando para iniciar la sesión para el script de la herramienta de pruebas:

```
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: Generar resultados

El script de la herramienta de pruebas es un programa basado en Python que crea dinámicamente un script bash para generar resultados en función de los datos introducidos. Tiene flexibilidad para generar resultados basados en uno o más tipos de recursos de AWS, planes de protección de GuardDuty, [Propósitos de amenaza](#) (tácticas), [Orígenes de datos fundamentales](#), o [the section called “El script de la herramienta de pruebas de resultados de GuardDuty puede generar”](#).

Utilice los siguientes ejemplos de comandos como referencia y ejecute uno o varios comandos para generar los resultados que desee explorar:

```
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'
```

Para obtener más información sobre los parámetros válidos, puede ejecutar el siguiente comando de ayuda:

```
python3 guardduty_tester.py --help
```

Parte C: Revise los resultados generados

Elija el método que prefiera para ver los resultados generados en la cuenta.

GuardDuty console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Resultados.

3. En la tabla de resultados, seleccione el resultado del que desea ver los detalles. Se abrirá el panel de detalles del resultado. Para obtener más información, consulte [Comprender y generar resultados de Amazon GuardDuty](#).
4. Si desea filtrar estos resultados, utilice la clave y el valor de la etiqueta del recurso. Por ejemplo, para filtrar los resultados generados para las instancias de Amazon EC2, utilice el par de clave y valor de etiqueta CreatedBy:GuardDuty Test Script para la Clave de etiqueta de instancia y Clave de etiqueta de instancia.

API

- Ejecute [ListFindings](#) para ver los resultados correspondientes a un ID de detector específico. Puede especificar parámetros para filtrar resultados.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

AWS CLI

- Ejecute el siguiente comando de la AWS CLI para ver los resultados generados y sustituya *us-east-1* y *12abc34d567e8fa901bc2d34EXAMPLE* por los valores adecuados:

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Para obtener más información sobre los parámetros que puede utilizar para filtrar los resultados, consulte [list-findings](#) en la Referencia de comandos de AWS CLI.

Paso 4: Limpiar los recursos de pruebas de AWS

La configuración a nivel de cuenta y otras actualizaciones del estado de la configuración realizadas durante [Paso 3: Ejecute los scripts de la herramienta de pruebas](#) vuelven al estado original cuando finaliza el script de la herramienta de pruebas.

Después de ejecutar el script de la herramienta de pruebas, podrá optar por limpiar los recursos de pruebas de AWS. Para ello, puede optar por uno de los siguientes métodos:

- Ejecuta el siguiente comando:

```
cdk destroy
```

- Elimine la pila CloudFormation con el nombre GuardDutyTesterStack. Para obtener información sobre los pasos, consulte [Eliminar una pila en la consola de CloudFormation](#).

Solución de problemas comunes

GuardDuty ha identificado problemas comunes y recomienda pasos para solucionarlos:

- `Cloud assembly schema version mismatch`: actualice la CLI de AWS CDK a una versión compatible con la versión de ensamblaje en la nube requerida, o a la versión más reciente disponible. Para obtener más información, consulte [Compatibilidad de la CLI con AWS CDK](#).
- `Docker permission denied`: agregue el usuario de la cuenta dedicada a los docker o docker-users de modo que la cuenta dedicada pueda ejecutar los comandos. Para obtener más información sobre los pasos, consulte la [opción de socket Daemon](#).
- `Your requested instance type is not supported in your requested Availability Zone`: algunas zonas de disponibilidad no admiten determinados tipos de instancias. Para identificar qué zonas de disponibilidad admiten el tipo de instancia de su preferencia y volver a intentar implementar recursos de AWS, siga los pasos que se indican a continuación:

1. Elija el método que prefiera para determinar qué zonas de disponibilidad admiten el tipo de instancia:

Console

Para identificar las zonas de disponibilidad que admiten el tipo de instancia de su preferencia

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Utilice el selector de regiones de AWS situado en la esquina superior derecha de la página para elegir la región en la que desea lanzar la instancia.
3. En el panel de navegación, en Instancias, seleccione Tipos de instancias.
4. Elija el tipo de instancia de su preferencia de la tabla Tipos de instancias.

5. En Redes, consulte las regiones enumeradas en Zonas de disponibilidad.

Según esta información, es posible que tenga que elegir una nueva región en la que implementar los recursos.

AWS CLI

Ejecute el siguiente comando para ver una lista de las zonas de disponibilidad. Asegúrese de especificar el tipo de instancia de su preferencia y la región (*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
```

Para obtener más información sobre este comando, consulte [describe-instance-type-offerings](#) en la Referencia de comandos de la AWS CLI.

Al ejecutar este comando, si se produce un error, asegúrese de que utiliza la versión más reciente de la AWS CLI. Para obtener más información, consulte [Solución de problemas](#) en la Guía del usuario de AWS Command Line Interface.

2. Intente volver a implementar los recursos de AWS y especifique una zona de disponibilidad que sea compatible con el tipo de instancia de su preferencia.

Para volver a intentar implementar los recursos de AWS

1. Configure la región predeterminada en el archivo `bin/cdk-gd-tester.ts`.
2. Para especificar la zona de disponibilidad, abra el archivo `amazon-guardduty-tester/lib/common/network/vpc.ts`.
3. En este archivo, sustituya `maxAzs: 2`, por `availabilityZones: ['us-east-1a', 'us-east-1c']`, donde debe especificar las zonas de disponibilidad para el tipo de instancia.
4. Continúe con los pasos restantes en [Pasos para implementar recursos de AWS](#).

Ver los resultados generados en la consola de GuardDuty

Cuando GuardDuty detecta una actividad que coincide con el patrón de un problema de seguridad, GuardDuty genera un resultado. Este resultado está asociado a un tipo de recurso que puede

haberse visto comprometido durante esta actividad. Puede ver los detalles asociados a cada tipo de resultado que GuardDuty genera.

Si utiliza una cuenta de administrador de GuardDuty, puede ver los resultados generados en nombre de las cuentas de miembro. Sin embargo, una cuenta de miembro puede ver los resultados generados en su propia cuenta. Una cuenta de miembro no puede ver los resultados generados por otras cuentas de miembro.

Pasos para ver los resultados en la consola de GuardDuty

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación izquierdo, elija Resultados.

GuardDuty muestra los resultados en formato tabular. De forma predeterminada, esta tabla se ordena en orden decreciente según el valor de la columna Vista por última vez y muestra los resultados más recientes en la parte superior.

Los resultados con el icono de una espada



representan un resultado de la secuencia de ataque.

3. Para ver los detalles asociados a un resultado, seleccione su título. Se abrirá el panel lateral de detalles del resultado. Para los resultados de una secuencia de ataque, este panel lateral incluye una versión resumida de la secuencia de ataque y, para ampliar esta vista, seleccione Ver detalles.

Para obtener información acerca de los campos que aparecen en este panel lateral, consulte [Detalles de los resultados](#).

4. (Opcional) para descargar resultados JSON
 - a. Seleccione el resultado y, a continuación, elija el menú Acciones.
 - b. En el menú Acciones, elija Exportar.
 - c. En la ventana Resultados JSON, seleccione Descargar.

Note

En algunos casos, GuardDuty se da cuenta de que algunos resultados son falsos positivos una vez que se han generado. GuardDuty proporciona un campo

Confianza en el JSON del resultado y establece su valor en cero. De esta forma, GuardDuty le permite saber que puede ignorar estos resultados de forma segura. Los resultados sin el campo Confianza no se consideran falsos positivos.

Navegación en la página Resultados

Esta sección proporciona información clave sobre varios elementos de la página Resultados. Esto le ayudará a analizar los resultados generados para analizar las amenazas y responder a ellas.

En la siguiente lista se explican los elementos de la página Resultados que le ayudarán a comprender mejor los resultados generados:

- Tipo de amenaza:

El tipo de amenaza incluye los resultados individuales de GuardDuty y los resultados de la secuencia de ataque. De forma predeterminada, la página muestra Todos los resultados.

Para filtrar la vista de la tabla de resultados, en el menú Tipo de amenaza, seleccione una de las opciones: Solo resultados de la secuencia de ataque o Solo resultados individuales.

- Columnas de recursos y recuento:

La columna Recursos de la tabla de resultados muestra el nombre del recurso de AWS potencialmente comprometido. En el caso de un resultado de una secuencia de ataque, esta columna muestra la cantidad de recursos de AWS potencialmente comprometidos. Para ver los nombres de los recursos, seleccione el número que aparece en la columna Recurso.

La columna Recuento indica el número de veces que GuardDuty observa un resultado específico. Cuando GuardDuty detecta una actividad que coincide con un problema de seguridad identificado anteriormente, aumenta el recuento de ese resultado específico. En el caso de un resultado de la secuencia de un ataque, el valor de esta columna indica el número total de señales y resultados involucrados en la generación del resultado.

- Clasificación de los resultados por columnas de la tabla:

Si hay una flecha junto al encabezado de una columna, puede ordenar la tabla de resultados en función de la columna. Seleccione el encabezado de la columna para ordenar los resultados en orden creciente o decreciente según el valor de esa columna.

- Filtrado de resultados:

En función de atributos de propiedad específicos, como Account ID y Resource type, puede filtrar aún más la tabla de resultado. Para obtener más información sobre los tipos de filtros que puede utilizar, consulte [Filtrar los resultados de GuardDuty](#).

- Reglas de estado y guardadas:

El menú Estado incluye dos valores: Actual y Archivado. La vista predeterminada es resultados actuales en la tabla.

Cuando ya no desee que GuardDuty genere un resultado que coincida con un criterio específico, puede suprimir ese resultado. GuardDuty archiva ese resultado. Cuando GuardDuty vuelva a detectar este resultado, no se le notificará esta observación. Para ver específicamente los resultados archivados, en el menú de estado, seleccione Archivado.

Las reglas guardadas son una característica que le ayuda a filtrar automáticamente los resultados que coinciden con un criterio específico y a tomar medidas al respecto. Las acciones pueden incluir archivar los resultados o suprimirlos de futuras notificaciones.

Para obtener más información, consulte [Reglas de supresión](#).

Niveles de gravedad de los resultados de GuardDuty

Cada resultado de GuardDuty tiene asignado un nivel de gravedad y un valor que refleja el riesgo potencial que el resultado podría tener para su entorno según lo determinado por nuestros ingenieros de seguridad. El valor de la gravedad puede estar comprendido en cualquier lugar dentro del intervalo de 1,0 a 10,0, donde los valores superiores indican un mayor riesgo de seguridad. Para ayudarle a determinar una respuesta a un posible problema de seguridad resaltado por un resultado, GuardDuty desglosa este intervalo en niveles de gravedad: Crítica, Alta, Media y Baja.

Un resultado de un tipo concreto puede tener una gravedad diferente según el contexto específico de dicho resultado. Para ver una lista consolidada de los niveles de gravedad predeterminados para todos los tipos de resultados de GuardDuty, consulte [Tipos de resultados activos de GuardDuty](#).

En las siguientes secciones se explican los niveles de gravedad definidos para los resultados de GuardDuty.

Temas

- [Gravedad crítica](#)

- [Gravedad alta](#)
- [Gravedad media](#)
- [Gravedad baja](#)

Gravedad crítica

Rango de valores: 9,0 - 10,0

Descripción: un nivel de gravedad crítico indica que una secuencia de ataque puede estar en curso o haber ocurrido recientemente. Uno o más recursos de AWS, como las credenciales de inicio de sesión de los usuarios de IAM y el bucket de Amazon S3, pueden estar en peligro o ya lo están.

Recomendación: GuardDuty recomienda priorizar la clasificación y la corrección de todos los resultados de gravedad crítica, ya que estos problemas pueden formar parte de un ataque de ransomware y pueden agravarse en cualquier momento. Consulte los detalles sobre los recursos involucrados y comience a abordar los problemas de seguridad. Para obtener más información, consulte [Corrección de resultados](#).

Gravedad alta

Rango de valores: 7,0 - 8,9

Descripción: un nivel de seguridad alto indica que el recurso en cuestión (una instancia de Amazon EC2 o un conjunto de credenciales de inicio de sesión de usuarios de IAM) está en peligro y que se está utilizando activamente para fines no autorizados.

Recomendación: GuardDuty recomienda que trate cualquier problema de seguridad alto con un resultado de gravedad alta como una prioridad y que tome medidas de corrección inmediatas para evitar el uso no autorizado de sus recursos. Por ejemplo, limpie la instancia de Amazon EC2 o térmela, o rote las credenciales de IAM. Siga los pasos que se indican [Corrección de resultados](#) para corregir el resultado.

Gravedad media

Rango de valores: 4,0 - 6,9

Descripción: un nivel de gravedad mediano indica una actividad sospechosa que se desvía del comportamiento observado normalmente y, en función de su caso de uso, puede ser indicativo de un peligro para los recursos.

Recomendación: GuardDuty recomienda que investigue el recurso potencialmente afectado tan pronto como sea posible. Los pasos de corrección variarán según el recurso y la familia de resultados. Un enfoque establecido consiste en confirmar que la actividad está autorizada y es coherente con su caso de uso. Si no puede identificar la causa o confirmar que la actividad está autorizada, debería considerar el recurso como afectado. Siga los pasos que se indican [Corrección de resultados](#) para corregir el resultado.

Estas son algunas cosas a tener en cuenta al revisar un resultado de nivel mediano:

- Compruebe si un usuario autorizado ha instalado nuevo software que haya cambiado el comportamiento de un recurso (por ejemplo, permitir un tráfico superior al normal o habilitar la comunicación en un nuevo puerto).
- Verifique si un usuario autorizado cambió la configuración del plano de control; por ejemplo, si modificó la configuración de un grupo de seguridad.
- Ejecute un examen antivirus en el recurso implicado para detectar software no autorizado.
- Verifique los permisos asociados al rol de IAM, usuario, grupo o conjunto de credenciales implicados. Tal vez sea necesario cambiarlos o moverlos.

Gravedad baja

Rango de valores: 1,0 - 3,9

Descripción: un nivel de gravedad bajo indica un intento de actividad sospechosa que no puso en peligro el entorno; por ejemplo, un análisis de puerto o un intento fallido de intrusión.

Recomendación: no hay ninguna acción recomendada inmediata, pero vale la pena tomar nota de esta información ya que puede indicar que alguien busca puntos débiles en el entorno.

Detalles de los resultados

Puede ver los detalles de los resultados en la sección de resumen en la consola de Amazon GuardDuty. Los detalles de los resultados varían según el tipo de resultado.

Hay dos detalles principales que determinarán qué tipo de información está disponibles para cualquier resultado. El primero es el tipo de recurso, que puede ser Instance, AccessKey, S3Bucket, S3Object, Kubernetes cluster, ECS cluster, Container, RDSDBInstance, RDSLimitlessDB o Lambda. El segundo detalle que determina la información de los resultados

es el rol del recurso. El rol del recurso puede ser Target, lo que significa que el recurso fue el blanco de una actividad sospechosa. En el caso de resultados por tipo de instancia, el rol del recurso también puede ser Actor, lo que significa que el recurso fue el actor que ha llevado a cabo la actividad sospechosa. En este tema, se describen algunos de los detalles de los resultados que se encuentran disponibles con más frecuencia. Para [the section called “Tipos de resultados de la supervisión en tiempo de ejecución”](#) y [Tipo de resultado de la protección contra malware para S3](#), no se ha completado el rol del recurso.

Temas

- [Información general de los resultados](#)
- [Recurso](#)
- [Detalles de los resultados de la secuencia de ataque](#)
- [Detalles de usuario de la base de datos \(DB\) de RDS](#)
- [Detalles del resultado de la supervisión en tiempo de ejecución](#)
- [Detalles del análisis de volúmenes de EBS](#)
- [Detalles de los resultados de Malware Protection for EC2](#)
- [Detalles de los resultados de la protección contra malware para S3](#)
- [Acción](#)
- [Actor u objetivo](#)
- [Detalles de geolocalización](#)
- [Información adicional](#)
- [Evidencia](#)
- [Comportamiento anómalo](#)

Información general de los resultados

La sección Información general de un resultado contiene las características identificativas más básicas del resultado, incluida la siguiente información:

- ID de cuenta: el ID de la cuenta de AWS en la que se llevó a cabo la actividad que indicó a GuardDuty la generación del resultado.
- Recuento: el número de veces que GuardDuty ha agregado una actividad que hace coincidir este patrón con este ID de resultado.

- Hora de creación: fecha y hora en que se ha creado este resultado por primera vez. Si este valor difiere de Hora de actualización, indica que la actividad se ha producido varias veces y es un problema continuo.

 Note

Las marcas de tiempo de los resultados de la consola de GuardDuty se muestran según la zona horaria local, mientras que las exportaciones JSON y las salidas de la CLI muestran las marcas de tiempo en UTC.

- ID de resultado: un identificador único para este tipo de resultado y conjunto de parámetros. Las nuevas ocurrencias de actividad que coincidan con este patrón se añadirán al mismo ID.
- Tipo de resultado: una cadena formateada que representa el tipo de actividad que ha desencadenado el resultado. Para obtener más información, consulte [Formato de resultado de GuardDuty](#).
- Región: la región de AWS en la que se ha generado el resultado. Para obtener más información acerca de las regiones admitidas, consulte [Regiones y puntos de conexión](#).
- ID de recurso: el ID del recurso de AWS en el que tuvo lugar la actividad que indicó a GuardDuty la generación del resultado.
- ID de análisis: se aplica a los resultados cuando la protección contra malware de GuardDuty para EC2 está habilitada, es un identificador del análisis de malware que se ejecuta en los volúmenes de EBS asociados a la instancia o carga de trabajo de contenedores de EC2 potencialmente comprometida. Para obtener más información, consulte [Detalles de los resultados de Malware Protection for EC2](#).
- Gravedad: un nivel de gravedad crítica, alta, mediana o baja asignado al resultado. Para obtener más información, consulte [Niveles de gravedad de los resultados](#).
- Hora de actualización: la última vez que se actualizó este resultado con una nueva actividad que coincidía con el patrón que llevó a GuardDuty a generar este resultado.

Recurso

El Recurso afectado proporciona detalles sobre el recurso de AWS donde se llevó a cabo la actividad desencadenante. La información disponible variará según el tipo de recurso y el tipo de acción.

Rol del recurso: el rol del recurso de AWS que inició el resultado. Este valor puede ser TARGET o ACTOR y representa si su recurso era el objetivo de la actividad sospechosa o si era el actor que ha llevado a cabo la actividad sospechosa, respectivamente.

Tipo de recurso: el tipo del recurso afectado. Si estuvieron involucrados varios recursos, un resultado puede incluir varios tipos de recursos. Los tipos de recursos son Instance, AccessKey, S3Bucket, S3Object, KubernetesCluster, ECSCluster, Container, RDSDBInstance, RDSLimitlessDB y Lambda. En función del tipo de recurso, habrá distintos detalles disponibles sobre el resultado. Seleccione una pestaña de opciones de recurso para obtener información sobre los detalles disponibles de ese recurso.

Instance

Detalles de la instancia:

Note

Es posible que falten algunos detalles de la instancia si esta ya se ha detenido o si la invocación a la API subyacente se ha originado en una instancia de EC2 en una región diferente al hacer una llamada a la API entre regiones.

- **ID de instancia:** el ID de la instancia de EC2 implicada en la actividad que indicó a GuardDuty la generación del resultado.
- **Tipo de instancia:** el tipo de instancia de EC2 implicada en el resultado.
- **Hora de lanzamiento:** la fecha y hora en que se lanzó la instancia.
- **ARN de Outpost:** el nombre de recurso de Amazon (ARN) de AWS Outposts. Solo se aplica a las instancias AWS Outposts. Para obtener más información, consulte [¿Qué es AWS Outposts?](#) en la Guía del usuario de bastidores Outposts.
- **Nombre del grupo de seguridad:** el nombre del grupo de seguridad asociado a la instancia en cuestión.
- **ID del grupo de seguridad:** el ID del grupo de seguridad asociado a la instancia en cuestión.
- **Estado de la instancia:** el estado actual de la instancia afectada.
- **Zona de disponibilidad:** la zona de disponibilidad de la región de AWS en la que se encuentra la instancia en cuestión.
- **ID de imagen:** el ID de la imagen de máquina de Amazon utilizada para crear la instancia implicada en la actividad.

- Descripción de la imagen: una descripción del ID de la imagen de máquina de Amazon utilizada para crear la instancia implicada en la actividad.
- Etiquetas: una lista de etiquetas adjuntas a este recurso, enumeradas en el formato de key-value.

AccessKey

Detalles de la clave de acceso:

- ID de clave de acceso: el ID de la clave de acceso del usuario implicado en la actividad que indicó a GuardDuty la generación del resultado.
- ID de entidad principal: el ID de entidad principal del usuario implicado en la actividad que indicó a GuardDuty la generación del resultado.
- Tipo de usuario: el tipo de usuario implicado en la actividad que indicó a GuardDuty la generación del resultado. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- Nombre de usuario: el nombre del usuario implicado en la actividad que indicó a GuardDuty la generación del resultado.

S3Bucket

Detalles del bucket de Amazon S:

- Nombre: el nombre del bucket implicado en el resultado.
- ARN: el ARN del bucket implicado en el resultado.
- Propietario: el ID canónico del usuario propietario del bucket implicado en el resultado. Para más información acerca de los ID de usuario canónico, consulte [AWS account identifiers](#).
- Tipo: el tipo de resultado del bucket, que puede ser de Destino o de Origen.
- Cifrado predeterminado del servidor: los detalles de cifrado del bucket.
- Etiquetas del bucket: una lista de etiquetas asociadas a este recurso, enumeradas en el formato de key-value.
- Permisos efectivos: una evaluación de todos los permisos y políticas efectivos del bucket que indica si el bucket en cuestión está expuesto públicamente. Los valores pueden ser Público o No público.

S3Object

- Detalles del objeto de S3: incluye la siguiente información sobre el objeto de S3 analizado:
 - ARN: nombre de recurso de Amazon (ARN) del objeto de S3 analizado.
 - Clave: el nombre asignado al archivo cuando se creó en el bucket de S3.
 - ID de versión: si ha habilitado el control de versiones del bucket, este campo indica el identificador de versión asociado a la versión más reciente del objeto de S3 analizado. Para obtener más información, consulte [Uso del control de versiones en buckets de S3](#) en la Guía de usuario de Amazon S3.
 - eTag: representa la versión específica del objeto de S3 analizado.
 - Hash: hash de la amenaza detectada en este resultado.
- Detalles del bucket de S3: incluye la siguiente información sobre el bucket de Amazon S3 asociado al objeto de S3 analizado:
 - Nombre: indica el nombre del bucket de S3 que contiene el objeto.
 - ARN: el nombre de recurso de Amazon (ARN) del bucket de S3.
 - Propietario: ID canónico del propietario del bucket de S3.

EKSCluster

Detalles del clúster de Kubernetes:

- Nombre: el nombre del clúster de Kubernetes.
- ARN: el ARN que identifica al clúster.
- Hora de creación: fecha y hora en que se ha creado este clúster.



Note

Las marcas de tiempo de los resultados de la consola de GuardDuty se muestran según la zona horaria local, mientras que las exportaciones JSON y las salidas de la CLI muestran las marcas de tiempo en UTC.

- ID de VPC: el ID de la VPC asociada al clúster.
- Estado: el estado actual del clúster.

- **Etiquetas:** los metadatos que se aplican a los clústeres para ayudarle a categorizarlos y organizarlos. Cada etiqueta consta de una clave y un valor opcional, mostrada en el formato `key-value`. Puede definir tanto la clave como el valor.

Las etiquetas del clúster no se propagan a ningún otro recurso asociado al clúster.

Detalles de la carga de trabajo de Kubernetes:

- **Tipo:** el tipo de carga de trabajo de Kubernetes, como el pod, la implementación y el trabajo.
- **Nombre:** el nombre de la carga de trabajo de Kubernetes.
- **Uid:** el ID único de la carga de trabajo de Kubernetes.
- **Hora de creación:** fecha y hora en que se ha creado esta carga de trabajo.
- **Etiquetas:** los pares de clave-valor asociados a la carga de trabajo de Kubernetes.
- **Contenedores:** los detalles del contenedor que se ejecuta como parte de la carga de trabajo de Kubernetes.
- **Espacio de nombres:** la carga de trabajo pertenece a este espacio de nombres de Kubernetes.
- **Volúmenes:** los volúmenes que utiliza la carga de trabajo de Kubernetes.
 - **Ruta del host:** representa un archivo o directorio preexistente en la máquina host al que se asigna el volumen.
 - **Nombre:** el nombre del volumen.
- **Contexto de seguridad del pod:** define la configuración de privilegios y control de acceso para todos los contenedores de un pod.
- **Red de host:** se establece como `true` si los pods se han incluido en la carga de trabajo de Kubernetes.

Detalles de usuario de Kubernetes:

- **Grupos:** grupos de RBAC (control basado en el acceso a roles) de Kubernetes del usuario que ha participado en la actividad que generó el resultado.
- **ID:** el ID única del usuario de Kubernetes.
- **Nombre de usuario:** nombre del usuario de Kubernetes que ha participado en la actividad que generó el resultado.
- **Nombre de sesión:** entidad que ha asumido el rol de IAM con los permisos de RBAC de Kubernetes.

ECSCluster

Detalles del clúster de ECS:

- ARN: el ARN que identifica al clúster.
- Nombre: el nombre del clúster.
- Estado: el estado actual del clúster.
- Recuento de servicios activos: la cantidad de servicios que se ejecutan en el clúster en un estado ACTIVE. Puede ver estos servicios con [ListServices](#)
- Recuento de instancias de contenedor registradas: el número de instancias de contenedor registradas en el clúster. Esto incluye las instancias de contenedor tanto en estado ACTIVE como DRAINING.
- Recuento de tareas en ejecución: el número de tareas del clúster que se encuentran en estado RUNNING.
- Etiquetas: los metadatos que se aplican a los clústeres para ayudarle a categorizarlos y organizarlos. Cada etiqueta consta de una clave y un valor opcional, mostrada en el formato key-value. Puede definir tanto la clave como el valor.
- Contenedores: los detalles sobre el contenedor asociado a la tarea:
 - Nombre del contenedor: el nombre del contenedor.
 - Imagen del contenedor: la imagen del contenedor.
- Detalles de la tarea: los detalles de una tarea en un clúster.
 - ARN: el nombre de recurso de Amazon (ARN) de la tarea.
 - ARN de definición: el nombre de recurso de Amazon (ARN) de la definición de tarea que crea esta.
 - Versión: el contador de versiones de la tarea.
 - Hora de creación de la tarea: la marca de tiempo de Unix en la que se ha creado la tarea.
 - Hora de inicio de la tarea: la marca de tiempo de Unix cuando se ha iniciado la tarea.
 - Tarea iniciada por: la etiqueta especificada cuando se inicia una tarea.

Container

Detalles del contenedor:

- Tiempo de ejecución del contenedor: el tiempo de ejecución del contenedor (por ejemplo, `docker` o `containerd`) utilizado para ejecutar el contenedor.
- ID: el ID de la instancia de contenedor o las entradas de ARN completas de la instancia de contenedor.
- Nombre: el nombre del contenedor.
- Imagen: la imagen de la instancia de contenedor.
- Monturas de volumen: lista de monturas de volumen de contenedores. Un contenedor puede montar un volumen en su sistema de archivos.
- Contexto de seguridad: el contexto de seguridad de contenedor define la configuración de privilegios y control de acceso de un contenedor.
- Detalles del proceso: describe los detalles del proceso asociado al resultado.

RDSDBInstance

Detalles de RDSDBInstance:

Note

Este recurso está disponible en los resultados de RDS Protection relacionados con la instancia de base de datos.

- ID de instancia de base de datos: el identificador asociado a la instancia de base de datos implicada en el resultado de GuardDuty.
- Motor: el nombre del motor de base de datos de la instancia de base de datos implicada en el resultado. Los valores posibles son `Compatible with Aurora MySQL` o `Compatible with Aurora PostgreSQL`.
- Versión del motor: la versión del motor de base de datos que ha participado en el resultado de GuardDuty.
- ID de clúster de base de datos: el identificador del clúster de base de datos que contiene el ID de instancia de base de datos implicada en el resultado de GuardDuty.
- ARN de instancia de base de datos: el ARN que identifica la instancia de base de datos implicada en el resultado de GuardDuty.

RDSLimitlessDB

Detalles de RDSLimitlessDB:

Este recurso está disponible en los resultados de RDS Protection relacionados con la versión de motor compatible de Limitless Database.

- Identificador del grupo de partición de base de datos: el nombre asociado al grupo de partición de base de datos Limitless.
- ID de recurso del grupo de partición de base de datos: el identificador de recursos del grupo de partición de base de datos dentro de la base de datos Limitless.
- ARN del grupo de partición de base de datos: nombre de recurso de Amazon (ARN) que identifica el grupo de partición de base de datos.
- Motor: el identificador de la base de datos Limitless implicada en los resultados.
- Versión de motor: la versión del motor de la base de datos Limitless.
- Identificador del clúster de base de datos: nombre del clúster de base de datos que forma parte de la base de datos Limitless.

Para obtener información sobre los detalles de usuario y de autenticación de la base de datos potencialmente afectada, consulte [Detalles de usuario de la base de datos \(DB\) de RDS](#).

Lambda

Detalles de la función de Lambda

- Nombre de la función: el nombre de la función de Lambda implicada en el resultado.
- Versión de la función: la versión de la función de Lambda implicada en el resultado.
- Descripción de la función: una descripción de la función de Lambda implicada en el resultado.
- ARN de la función: el nombre de recurso de Amazon (ARN) de la función de Lambda implicada en el resultado.
- ID de revisión: el ID de revisión de la versión de la función de Lambda.
- Rol: el rol de ejecución de la función de Lambda implicada en el resultado.
- Configuración de VPC: la configuración de Amazon VPC, que incluye el ID de VPC, el grupo de seguridad y los ID de subred asociados a la función de Lambda.
 - ID de VPC: el ID de Amazon VPC asociada a la función de Lambda implicada en el resultado.

- ID de subred: los ID de las subredes asociadas a la función de Lambda.
- Grupo de seguridad: el grupo de seguridad asociado a la función de Lambda implicada. Esto incluye el nombre del grupo de seguridad y el ID de grupo.
- Etiquetas: una lista de etiquetas adjuntas a este recurso, con el formato de pares de key-value.

Detalles de los resultados de la secuencia de ataque

GuardDuty proporciona detalles de cada resultado que genere en su cuenta. Estos detalles ayudan a entender los motivos del resultado. Esta sección se centra en los detalles relacionados con [Tipos de resultados de secuencias de ataque](#). Esto incluye información como los recursos potencialmente afectados, el cronograma de los eventos, los indicadores, las señales y los puntos de conexión involucrados en el resultado.

Para ver los detalles asociados a las señales detectadas por GuardDuty, consulte las secciones correspondientes de esta página.

En la consola GuardDuty, al seleccionar un resultado de secuencia de ataque, el panel lateral de detalles se divide en las siguientes pestañas:

- Descripción general: proporciona una vista compacta de los detalles de la secuencia de ataque, incluidas las señales, las tácticas de MITRE y los recursos potencialmente afectados.
- Señales: muestra una cronología de los eventos que intervienen en una secuencia de ataque.
- Recursos: proporciona información sobre los recursos potencialmente afectados o los recursos que están potencialmente en riesgo.

La siguiente lista proporciona descripciones asociadas a los detalles de resultados de la secuencia de ataque.

Señales de

Una señal podría ser una actividad de la API o un resultado que GuardDuty utiliza para detectar un resultado de secuencia de ataque. GuardDuty tiene en cuenta las señales débiles que no se presentan como una amenaza clara, las organiza y las correlaciona con los resultados generados individualmente. Para obtener más contexto, la pestaña Señales proporciona una cronología de las señales, según lo observado por GuardDuty.

Cada señal, que es un resultado de GuardDuty, tiene su propio nivel de gravedad y valor asignado. En la consola de GuardDuty, puede seleccionar cada señal para ver los detalles asociados.

Actores

Proporciona detalles sobre los actores de las amenazas en una secuencia de ataque. Para obtener más información, consulte [Actor](#) en Referencia de la API de Amazon GuardDuty.

puntos de conexión

Proporciona detalles sobre los puntos de conexión de la red que se utilizaron en esta secuencia de ataque. Para obtener más información, consulte [NetworkEndpoint](#) en Referencia de la API de Amazon GuardDuty. Para obtener información sobre cómo GuardDuty determina la ubicación, consulte [Detalles de geolocalización](#).

Indicadores

Incluye datos observados que coinciden con el patrón de un problema de seguridad. Estos datos especifican por qué en GuardDuty hay indicios de una actividad potencialmente sospechosa. Por ejemplo, cuando el nombre del indicador es HIGH_RISK_API, esto indica que se trata de una acción que suelen utilizar los actores de amenazas o de una acción delicada que puede tener un impacto potencial en una Cuenta de AWS, como acceder a las credenciales o modificar un recurso.

En la siguiente tabla se incluye una lista de indicadores potenciales y sus descripciones:

Nombre del indicador	Descripción
ATTACK_TACTIC	Las tácticas de MITRE, como Discovery e Impact.
ATTACK_TECHNIQUE	La técnica MITRE utilizada por el actor de la amenaza en una secuencia de ataque. Algunos ejemplos incluyen acceder a los recursos y utilizarlos de forma no deseada, y explotar las vulnerabilidades.
CRYPTOMINING_DOMAIN	Indica un nombre de dominio asociado a los grupos o a la infraestructura de minería de criptomonedas. Por ejemplo, las consultas de DNS o las conexiones a estos dominios desde entornos de contenedores o de Kubernetes pueden indicar una actividad de minería de criptomonedas no autorizada.

Nombre del indicador	Descripción
	Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo .
CRYPTOMINING_IP	Indica una dirección IP asociada a los grupos o a la infraestructura de minería de criptomonedas. Por ejemplo, las conexiones a estas direcciones desde entornos de contenedores o de Kubernetes pueden indicar una actividad de minería de criptomonedas no autorizada. Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo.
CRYPTOMINING_PROCESS	Indica un proceso identificado como software de minería de criptomonedas que se ejecuta en entornos de contenedores o de Kubernetes. Por ejemplo, estos procesos pueden consumir recursos de CPU excesivos. Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo.
HIGH_RISK_API	La API de AWS que incluye el nombre del Servicio de AWS y el eventName indica una acción que suelen utilizar los actores de amenazas o es una acción confidencial que puede tener un impacto potencial en una de ellas Cuenta de AWS, como el acceso a una credencial o la modificación de un recurso.
MALICIOUS_DOMAIN	Indica un nombre de dominio con información sobre posibles inteligencia de amenazas que indica una intención maliciosa. Por ejemplo, esto incluye los servidores de comando y control (C&C), los sitios de distribución de malware o los dominios de suplantación de identidad a los que se accede desde entornos de contenedores o de Kubernetes. Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo.

Nombre del indicador	Descripción
MALICIOUS_IP	La dirección IP tiene inteligencia de amenazas confirmada que indica una intención maliciosa.
MALICIOUS_PROCESS	Indica un proceso sospechoso de ser malicioso en función de la inteligencia de amenazas o el análisis del comportamiento. Por ejemplo, esto incluye malware conocido, puertas traseras o herramientas no autorizadas que se ejecutan en entornos de contenedores o de Kubernetes con intenciones maliciosas. Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo.
SUSPICIOUS_NETWORK	Se sabe que la red está asociada a puntajes de reputación bajos, como los proveedores de redes privadas virtuales (VPN) y los servicios proxy riesgosos.
SUSPICIOUS_PROCESS	Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo .
SUSPICIOUS_USER_AGENT	El agente de usuario está asociado a aplicaciones sospechosas o explotadas potencialmente conocidas, como los clientes de Amazon S3 y las herramientas de ataque.
TOR_IP	La dirección IP está asociada a un nodo de salida de Tor.
UNUSUAL_API_FOR_ACCOUNT	Indica que la API AWS se invocó de forma anómala, según la línea base histórica de la cuenta. Para obtener más información, consulte Comportamiento anómalo .
UNUSUAL_ASN_FOR_ACCOUNT	Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea de base histórica de la cuenta. Para obtener más información, consulte Comportamiento anómalo .

Nombre del indicador	Descripción
UNUSUAL_ASN_FOR_USER	Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte Comportamiento anómalo .

Tácticas de MITRE

Este campo especifica las tácticas de MITRE ATT&CK que el actor de la amenaza intenta utilizar a través de una secuencia de ataque. GuardDuty utiliza el marco de [MITRE ATT&ACK](#) que añade contexto a toda la secuencia de ataque. Los colores que utiliza la consola GuardDuty para especificar los fines de amenaza que ha utilizado el autor de la amenaza se alinean con los colores que indican [Niveles de gravedad de los resultados](#) crítico, alto, medio y bajo.

Indicadores de red

Los indicadores incluyen una combinación de valores de indicadores de red que explican por qué una red es indicativa de un comportamiento sospechoso. Esta sección es aplicable solo cuando el indicador incluye SUSPICIOUS_NETWORK o MALICIOUS_IP. El siguiente ejemplo muestra cómo se pueden asociar los indicadores de red a un indicador, donde:

- *AnyCompany* es un Sistema Autónomo (AS).
- TUNNEL_VPN, IS_ANONYMOUS y ALLOWS_FREE_ACCESS son los indicadores de la red.

```
...{
  "key": "SUSPICIOUS_NETWORK",
  "values": [{
    "AnyCompany": [
      "TUNNEL_VPN",
      "IS_ANONYMOUS",
      "ALLOWS_FREE_ACCESS"
    ]
  }]
}
```

En la siguiente tabla se incluyen los valores de los indicadores de red y su descripción. Estas etiquetas se añaden en función de la inteligencia de amenazas que GuardDuty recopila de fuentes como Spur.

Valor de indicador de red	Descripción
TUNNEL_VPN	La dirección IP o de red está asociada a un tipo de túnel VPN. Se refiere a un protocolo específico que ayuda a establecer una conexión segura y cifrada entre dos puntos a través de una red pública.
TUNNEL_PROXY	La dirección IP o de red está asociada a un tipo de túnel Proxy. Esto se refiere a un protocolo específico que ayuda a establecer una conexión a través de un servidor proxy.
TUNNEL_RDP	La dirección IP o de red está asociada al uso de un método de encapsulación del tráfico de escritorios remotos (RDP) dentro de otro protocolo para mejorar la seguridad, evitar las restricciones de la red o permitir el acceso remoto a través de firewalls.
IS_ANONYMOUS	La dirección IP o de red está asociada a un servicio anónimo o proxy conocido. Esto puede indicar posibles actividades sospechosas que se esconden detrás de redes anónimas.
KNOWN_THREAT_OPERATOR	La dirección IP o de red está asociada a un proveedor de túnel de riesgos conocido. Esto indica que se ha detectado actividad sospechosa en una dirección IP vinculada a una VPN, un proxy u otros servicios de tunelización que se utilizan con frecuencia con fines maliciosos.
ALLOWS_FREE_ACCESS	La dirección IP o de red está asociada a un operador de túnel que permite el acceso a su servicio sin necesidad de autenticación ni pago. También puede incluir cuentas de prueba o experiencias de uso limitado que ofrecen varios servicios en línea.
ALLOWS_CRYPTOCURRENCY	La dirección IP o de red está asociada a un proveedor de túneles (como una VPN o un servicio proxy) que acepta exclusivamente criptomonedas u otras monedas digitales como método de pago.
ALLOWS_TORRENTS	La dirección IP o de red está asociada a los servicios o las plataformas que permiten el tráfico de torrents. Estos servicios suelen estar

Valor de indicador de red	Descripción
	relacionados con el apoyo y el uso de torrents y con actividades de evasión de derechos de autor.
RISK_CALL BACK_PROXY	La dirección IP o de red está asociada a dispositivos conocidos por enrutar el tráfico a servidores proxy residenciales, servidores proxy de malware u otras redes tipo proxy de devolución de llamadas. Esto no implica que toda la actividad de la red esté relacionada con los servidores proxy, sino que la red tiene la capacidad de enrutar el tráfico en nombre de estas redes proxy.
RISK_GEO_ MISMATCH	Este indicador sugiere que el centro de datos o la ubicación del host de una red difieren de la ubicación esperada de los usuarios y dispositivos conectados a ella. Si el valor de este indicador no está presente, no significa que no haya discrepancia. Puede implicar que no hay datos suficientes para confirmar la discrepancia.
IS_SCANNER	La red o la dirección IP están asociadas a los intentos de inicio de sesión persistentes en los formularios web.
RISK_WEB_ SCRAPING	La red de direcciones IP está asociada a los clientes web automatizados y a otras actividades web programáticas.
CLIENT_BE HAVIOR_FI LE_SHARING	La red o la dirección IP están asociadas al comportamiento del cliente, lo que indica actividades de intercambio de archivos, como las redes punto a punto (P2P) o los protocolos de intercambio de archivos.
CATEGORY_ COMMERCIA L_VPN	La red o la dirección IP están asociadas a un operador de túnel que se clasifica como un servicio de red privada virtual (VPN) comercial tradicional que opera dentro del espacio del centro de datos.
CATEGORY_ FREE_VPN	La red o la dirección IP están asociadas a un operador de túnel que se clasifica como un servicio de VPN completamente gratuito.
CATEGORY_ RESIDENTI AL_PROXY	La red o la dirección IP están asociadas a un operador de túnel que se clasifica como un SDK, un malware o un servicio proxy de origen gratuito.

Valor de indicador de red	Descripción
OPERATOR_XXX	El nombre del proveedor de servicios que opera este túnel.

Detalles de usuario de la base de datos (DB) de RDS

Note

Esta sección se aplica a los resultados cuando se habilita la característica de protección de RDS en GuardDuty. Para obtener más información, consulte [Protección de RDS de GuardDuty](#).

El resultado de GuardDuty proporciona los siguientes detalles de usuario y de autenticación de la base de datos potencialmente afectada:

- Usuario: el nombre de usuario utilizado para llevar a cabo el intento de inicio de sesión anómalo.
- Aplicación: el nombre de la aplicación utilizada para llevar a cabo el intento de inicio de sesión anómalo.
- Base de datos: el nombre de la instancia de base de datos implicada en el intento de inicio de sesión anómalo.
- SSL: la versión de capa de sockets seguros (SSL) utilizada para la red.
- Método de autenticación: el método de autenticación utilizado por el usuario implicado en el resultado.

Para obtener información acerca del recurso potencialmente afectado, consulte [Recurso](#).

Detalles del resultado de la supervisión en tiempo de ejecución

Note

Es posible que estos detalles solo estén disponibles si GuardDuty genera uno de los [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#).

Esta sección contiene los detalles del tiempo de ejecución, como los detalles del proceso y cualquier contexto necesario. Los detalles del proceso describen información sobre el proceso observado, y el contexto de ejecución describe cualquier información adicional sobre la actividad potencialmente sospechosa.

Detalles del proceso

- Nombre: el nombre del proceso.
- Ruta ejecutable: la ruta absoluta del archivo ejecutable del proceso.
- SHA-256 ejecutable: el hash SHA256 del ejecutable del proceso.
- PID del espacio de nombres: el ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID del host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
- Directorio de trabajo actual: el directorio de trabajo actual del proceso.
- ID del proceso: el ID asignado al proceso por el sistema operativo.
- startTime: la hora en la que se ha iniciado el proceso. Está en formato de cadena de fecha UTC (2023-03-22T19:37:20.168Z).
- UUID: el ID único asignado al proceso por GuardDuty.
- UUID principal: el ID único del proceso principal. GuardDuty asigna este ID al proceso principal.
- Usuario: el usuario que ha ejecutado el proceso.
- ID del usuario: el ID del usuario que ha ejecutado el proceso.
- ID del usuario efectivo: el ID del usuario efectivo del proceso en el momento del evento.
- Linaje: información sobre los antepasados del proceso.
 - ID del proceso: el ID asignado al proceso por el sistema operativo.
 - UUID: el ID único asignado al proceso por GuardDuty.
 - Ruta ejecutable: la ruta absoluta del archivo ejecutable del proceso.
 - ID del usuario efectivo: el ID del usuario efectivo del proceso en el momento del evento.
 - UUID principal: el ID único del proceso principal. GuardDuty asigna este ID al proceso principal.
 - Hora de inicio: la hora en la que se ha iniciado el proceso.
 - PID del espacio de nombres: el ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID del host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
 - ID del usuario: el ID del usuario que ejecutó el proceso.

- Nombre: el nombre del proceso.

Contexto del tiempo de ejecución

De los siguientes campos, un resultado generado puede incluir solo los campos que son relevantes para el tipo de resultado.

- Origen de la montura: la ruta en el host que monta el contenedor.
- Destino de la montura: la ruta del contenedor que está asignada al directorio del host.
- Tipo de sistema de archivos: representa el tipo de sistema de archivos montado.
- Marcas: representan las opciones que controlan el comportamiento del evento implicado en este resultado.
- Proceso de modificación: información sobre el proceso que ha creado o modificado un binario, un script o una biblioteca dentro de un contenedor en tiempo de ejecución.
- Modificado el: la marca de tiempo en la que el proceso ha creado o modificado un binario, un script o una biblioteca dentro de un contenedor en tiempo de ejecución. Este campo está en formato de cadena de fecha UTC (2023-03-22T19:37:20.168Z).
- Ruta de la biblioteca: la ruta a la nueva biblioteca que se ha cargado.
- Valor de precarga de LD: el valor de la variable de entorno LD_PRELOAD.
- Ruta del socket: la ruta al socket de Docker al que se accedió.
- Ruta al binario Runc: la ruta al binario `runc`.
- Ruta del agente de lanzamiento: la ruta al archivo del agente de lanzamiento del `cgroup`.
- Ejemplo de línea de comandos: ejemplo de la línea de comandos implicada en la actividad potencialmente sospechosa.
- Categoría de herramienta: categoría a la que pertenece la herramienta. Algunos ejemplos son las herramientas de puerta trasera, prueba de penetración, analizador de red y rastreador de red.
- Nombre de la herramienta: el nombre de la herramienta potencialmente sospechosa.
- Ruta del script: la ruta al script ejecutado que generó el resultado.
- Ruta del archivo de amenazas: la ruta sospechosa en la que se encontraron los detalles de la inteligencia de amenazas.
- Nombre del servicio: el nombre del servicio de seguridad que se ha desactivado.
- Nombre del módulo: nombre del módulo que se carga en el kernel.

- Módulo SHA256: el hash SHA256 del módulo.
- Ruta del archivo del módulo: ruta del módulo cargado en el kernel.

Detalles del análisis de volúmenes de EBS

Note

Esta sección se aplica a los resultados cuando se activa el análisis de malware iniciado por GuardDuty en [Protección contra malware para EC2](#).

El análisis de volúmenes de EBS proporciona detalles sobre el volumen de EBS asociado a la carga de trabajo del contenedor o la instancia de EC2 potencialmente afectada.

- ID de análisis: el identificador del análisis de malware.
- Análisis iniciado el: la fecha y hora en que inició el análisis de malware.
- Análisis completado el: la fecha y la hora en que se completó el análisis de malware.
- ID de resultado desencadenador: el ID del resultado de GuardDuty que inició este análisis de malware.
- Orígenes: los valores potenciales son Bitdefender y Amazon.

Para obtener más información sobre el motor de análisis utilizado para detectar malware, consulte [Motor de análisis de detección de malware de GuardDuty](#).

- Detecciones de análisis: la vista completa de los detalles y los resultados de cada análisis de malware.
 - Recuento de elementos analizados: el número total de archivos analizados. Proporciona detalles como `totalGb`, `files` y `volumes`.
 - Recuento de elementos de amenazas detectadas: el número total de files maliciosos detectados durante el análisis.
 - Detalles de las amenazas de mayor gravedad: los detalles de la amenaza de mayor gravedad detectada durante el análisis y el número de archivos maliciosos. Proporciona detalles como `severity`, `threatName` y `count`.
 - Amenazas detectadas por nombre: el elemento del contenedor que agrupa las amenazas de todos los niveles de gravedad. Proporciona detalles como `itemCount`, `uniqueThreatNameCount`, `shortened` y `threatNames`.

Detalles de los resultados de Malware Protection for EC2

Note

Esta sección se aplica a los resultados cuando se activa el análisis de malware iniciado por GuardDuty en [Protección contra malware para EC2](#).

Cuando el análisis de Malware Protection for EC2 detecta malware, podrá ver los detalles del análisis al seleccionar el resultado correspondiente en la página Resultados de la consola <https://console.aws.amazon.com/guardduty/>. La gravedad del resultado de Malware Protection for EC2 depende de la gravedad del resultado de GuardDuty.

La siguiente información está disponible en la sección Amenazas detectadas del panel de detalles.

- Nombre: el nombre de la amenaza, obtenido al agrupar los archivos por detección.
- Gravedad: el nivel de gravedad de la amenaza detectada.
- Hash: el SHA-256 del archivo.
- Ruta de archivo: la ubicación del archivo malicioso en el volumen de EBS.
- Nombre de archivo: el nombre del archivo en el que se detectó la amenaza.
- ARN del volumen: el ARN de los volúmenes de EBS analizados.

La siguiente información está disponible en la sección Detalles del análisis de malware del panel de detalles.

- ID de análisis: el ID del análisis de malware.
- Análisis iniciado el: la fecha y hora en que inició el análisis.
- Análisis completado el: la fecha y la hora en que se completó el análisis.
- Archivos analizados: el número total de archivos y directorios analizados.
- Total de GB analizados: la cantidad de almacenamiento analizada durante el proceso.
- ID de resultado desencadenador: el ID del resultado de GuardDuty que inició este análisis de malware.
- La siguiente información está disponible en la sección Detalles del volumen del panel de detalles.
 - ARN del volumen: el nombre de recurso de Amazon (ARN) del volumen.
 - SnapshotARN: el ARN de la instantánea del volumen de EBS.

- Estado: el estado de análisis del volumen, como Running, Skipped y Completed.
- Tipo de cifrado: el tipo de cifrado utilizado en el volumen. Por ejemplo, CCMK.
- Nombre del dispositivo: el nombre del dispositivo. Por ejemplo, /dev/xvda.

Detalles de los resultados de la protección contra malware para S3

Los siguientes detalles de análisis de malware están disponibles al habilitar tanto GuardDuty como la protección contra malware para S3 en la Cuenta de AWS:

- Amenazas: una lista de las amenazas detectadas durante el análisis de malware.

Múltiples amenazas potenciales en archivos de archivo

Si tiene un archivo de archivo con varias amenazas potenciales, la protección contra malware para S3 solo informa de la primera amenaza detectada. Tras ello, el estado del análisis se marca como completo. GuardDuty genera el tipo de resultado asociado y también envía los eventos de EventBridge que genera. Para obtener más información sobre la supervisión de los análisis de objetos de Amazon S3 mediante los eventos de EventBridge, consulte el esquema de notificaciones de muestra correspondiente a THREATS_FOUND en [Producto del análisis del objeto S3](#).

- Ruta del elemento: una lista de rutas de elementos anidados y detalles del hash del objeto de S3 analizado.
- Ruta del elemento anidado: ruta del elemento del objeto de S3 analizado en el que se detectó la amenaza.

El valor de este campo solo estará disponible si el objeto de nivel superior es un archivo y si se detecta una amenaza dentro de un archivo.

- Hash: hash de la amenaza detectada en este resultado.
- Orígenes: los valores potenciales son Bitdefender y Amazon.

Para obtener más información sobre el motor de análisis utilizado para detectar malware, consulte [Motor de análisis de detección de malware de GuardDuty](#).

Acción

La acción de un resultado proporciona detalles sobre el tipo de actividad que desencadenó el resultado. La información disponible variará en función del tipo de acción.

Tipo de acción: el tipo de actividad del resultado. Este valor puede ser `NETWORK_CONNECTION`, `PORT_PROBE`, `DNS_REQUEST`, `AWS_API_CALL` o `RDS_LOGIN_ATTEMPT`. La información disponible variará en función del tipo de acción:

- **NETWORK_CONNECTION:** indica que hubo un intercambio de tráfico de la red entre la instancia de EC2 identificada y el host remoto. Este tipo de acción presenta la siguiente información adicional:
 - **Dirección de conexión:** la dirección de la conexión de red observada en la actividad que solicitó a GuardDuty la generación del resultado. Puede ser uno de los siguientes valores:
 - **INBOUND:** indica que un host remoto inició una conexión con un puerto local en la instancia de EC2 identificada en su cuenta.
 - **OUTBOUND:** indica que la instancia de EC2 identificada inició una conexión a un host remoto.
 - **UNKNOWN** indica que GuardDuty no pudo determinar la dirección de la conexión.
 - **Protocolo:** el protocolo de conexión de red observado en la actividad que solicitó a GuardDuty la generación del resultado.
 - **IP local:** la dirección IP de origen original del tráfico que activó el resultado. Se puede usar esta información para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico que desencadenó la búsqueda. Por ejemplo, la dirección IP de un pod EKS en lugar de la dirección IP de la instancia en la que se ejecuta el pod EKS.
 - **Bloqueado:** indica si el puerto objetivo está bloqueado.
- **PORT_PROBE:** indica que un host remoto sondeó la instancia de EC2 identificada en varios puertos abiertos. Este tipo de acción presenta la siguiente información adicional:
 - **IP local:** la dirección IP de origen original del tráfico que activó el resultado. Se puede usar esta información para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico que desencadenó la búsqueda. Por ejemplo, la dirección IP de un pod EKS en lugar de la dirección IP de la instancia en la que se ejecuta el pod EKS.
 - **Bloqueado:** indica si el puerto objetivo está bloqueado.

- **DNS_REQUEST**: indica que la instancia de EC2 identificada consultó un nombre de dominio. Este tipo de acción presenta la siguiente información adicional:
 - **Protocolo**: el protocolo de conexión de red observado en la actividad que solicitó a GuardDuty la generación del resultado.
 - **Bloqueado**: indica si el puerto objetivo está bloqueado.
- **AWS_API_CALL**: indica que se ha invocado una API de AWS. Este tipo de acción presenta la siguiente información adicional:
 - **API**: el nombre de la operación de API a la que se invocó y que solicitó a GuardDuty la generación de este resultado.

 Note

Estas operaciones también pueden incluir eventos que no pertenecen a la API capturados por AWS CloudTrail. Para más información, consulte [Non-API events captured by CloudTrail](#).

- **Agente de usuario**: el agente de usuario que hizo la solicitud de API. Este valor indica si la llamada se hizo desde la Consola de administración de AWS, un servicio de AWS, los AWS SDK o la AWS CLI.
- **CÓDIGO DE ERROR**: si una llamada fallida a la API ha desencadenado el resultado, se muestra el código de error de esa llamada.
- **Nombre del servicio**: el nombre de DNS del servicio que ha intentado hacer la llamada a la API que desencadenó el resultado.
- **RDS_LOGIN_ATTEMPT**: indica que se intentó iniciar sesión en la base de datos potencialmente afectada desde una dirección IP remota.
 - **Dirección IP**: la dirección IP remota que se utilizó para llevar a cabo el intento de inicio de sesión potencialmente sospechoso.

Actor u objetivo

Un resultado tendrá una sección Actor si el Rol de recurso era TARGET. Esto indica que su recurso fue objeto de actividad sospechosa y la sección Actor contendrá detalles sobre la entidad que tenía el recurso como objetivo.

Un resultado tendrá una sección Objetivo si el Rol de recurso era ACTOR. Esto indica que su recurso estuvo involucrado en actividad sospechosa contra un host remoto y esta sección contendrá información sobre la IP o el dominio que era el objetivo de su recurso.

La información disponible en la sección Actor u Objetivo puede incluir lo siguiente:

- **Afiliado:** detalles sobre si la cuenta de AWS de la persona que llama a la API remota está relacionada con su entorno de GuardDuty. Si este valor es `true`, la persona que llama a la API está afiliada a su cuenta de alguna manera; si es `false`, la persona que llama a la API es ajena a su entorno.
- **ID de cuenta remota:** el ID de cuenta propietaria de la dirección IP saliente que se utilizó para acceder al recurso en la red final.
- **Dirección IP:** la dirección IP implicada en la actividad que solicitó a GuardDuty la generación del resultado.
- **Ubicación:** la información de ubicación de la dirección IP implicada en la actividad que solicitó a GuardDuty la generación del resultado.
- **Organización:** la información de la organización de ISP de la dirección IP implicada en la actividad que solicitó a GuardDuty la generación del resultado.
- **Puerto:** el número del puerto implicado en la actividad que solicitó a GuardDuty la generación del resultado.
- **Dominio:** el dominio implicado en la actividad que solicitó a GuardDuty la generación del resultado.
- **Dominio con sufijo:** el dominio de segundo y primer nivel implicado en una actividad que posiblemente haya solicitado a GuardDuty la generación del resultado. Para obtener una lista de dominios de primer y segundo nivel, consulte la [lista de sufijos públicos](#).

Detalles de geolocalización

GuardDuty determina la ubicación de las solicitudes mediante las bases de datos GeoIP de MaxMind. MaxMind informa de una precisión muy alta de sus datos a nivel de país, aunque la precisión varía según factores como el país y el tipo de dirección IP.

Para obtener más información sobre MaxMind, consulte [Geolocalización IP de MaxMind](#). Si cree que alguno de los datos de GeoIP es incorrecto, puede enviar una solicitud de corrección a MaxMind en [Corregir datos GeoIP2 de MaxMind](#).

Información adicional

Todos los resultados tienen una sección de Información adicional donde se puede encontrar la siguiente información:

- **Nombre de la lista de amenazas:** el nombre de la lista de amenazas que incluye la dirección IP o el nombre de dominio implicado en la actividad para la que se solicitó a GuardDuty que generara el resultado.
- **Muestra:** un valor verdadero o falso que indica si se trata de un resultado de muestra.
- **Archivado:** un valor verdadero o falso que indica si el resultado se ha archivado.
- **Inusual:** detalles de las actividades que no se han observado históricamente. Pueden incluir cualquier usuario, hora, ubicación, bucket, comportamiento de inicio de sesión u organización de ASN inusuales (no observados previamente).
- **Protocolo inusual:** el protocolo de conexión de red implicado en la actividad que solicitó a GuardDuty la generación del resultado.
- **Detalles del agente:** detalles sobre el agente de seguridad que está implementado actualmente en el clúster de EKS de su Cuenta de AWS. Esto solo se aplica a los tipos de resultados de la Supervisión en tiempo de ejecución de EKS.
 - **Versión del agente:** la versión del agente de seguridad de GuardDuty.
 - **ID del agente:** el identificador único del agente de seguridad de GuardDuty.

Evidencia

Los resultados que se obtienen mediante la inteligencia sobre amenazas tienen una sección de Evidencia que incluye la siguiente información:

- **Detalles de inteligencia de amenazas:** el nombre de la lista de amenazas en la que aparece el `Threat name` reconocido.
- **Nombre de la amenaza:** el nombre de la familia de malware u otro identificador asociado a la amenaza.
- **Archivo de amenaza SHA256:** SHA256 del archivo que generó el resultado.

Comportamiento anómalo

Los tipos de resultados que terminan en `AnomalousBehavior` indican que el resultado se ha generado mediante el modelo de machine learning (ML) de detección de anomalías de GuardDuty. El modelo de ML evalúa todas las solicitudes de API a su cuenta e identifica los eventos anómalos relacionados con las tácticas utilizadas por los adversarios. El modelo de ML da seguimiento a varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó.

Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad del usuario de CloudTrail que ha invocado la solicitud se encuentran en los detalles del resultado. Las identidades las define el [elemento `userIdentity` de CloudTrail](#) y los valores posibles son: `Root`, `IAMUser`, `AssumedRole`, `FederatedUser`, `AWSAccount` o `AWSService`.

Además de los detalles disponibles para todos los resultados de GuardDuty asociados con la actividad de la API, los resultados de `AnomalousBehavior` tienen detalles adicionales que se describen en la siguiente sección. Estos detalles se pueden ver en la consola y también están disponibles en el JSON de los resultados.

- **API anómalas:** lista de solicitudes de API invocadas por la identidad del usuario cerca de la solicitud de API principal asociada al resultado. En este panel se desglosan en profundidad los detalles del evento de la API de las siguientes maneras.
 - La primera API de la lista es la API principal, que es la solicitud de API asociada a la actividad observada de mayor riesgo. Esta es la API que ha desencadenado el resultado y se correlaciona con la fase de ataque del tipo de resultado. Esta es también la API que se detalla en la sección **Acción** de la consola y en el JSON del resultado.
 - Todas las demás API de la lista son API anómalas adicionales a la identidad de usuario de la lista observadas cerca de la API principal. Si solo hay una API en la lista, el modelo de ML no ha identificado como anómala ninguna solicitud de API adicional procedente de esa identidad de usuario.
 - La lista de API se divide en función de si una API se llamó correctamente o si se llamó de forma incorrecta, lo que significa que se recibió una respuesta de error. El tipo de respuesta de error recibida aparece encima de cada API llamada incorrectamente. Los posibles tipos de respuesta de error son: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` y `operation not permitted`.
 - Las API se clasifican según su servicio asociado.

- Para obtener más contexto, seleccione API históricas para ver los detalles sobre las API principales, hasta un máximo de 20, que normalmente se muestran tanto para la identidad del usuario como para todos los usuarios de la cuenta. Las API se marcan como Raro (menos de una vez al mes), Poco frecuente (varias veces al mes) o Frecuente (diario o semanal), en función de la frecuencia con la que se usen en la cuenta.
- Comportamiento inusual (cuenta): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado de su cuenta.

Comportamiento perfilado

GuardDuty aprende continuamente sobre las actividades dentro de la cuenta en función de los eventos entregados. Estas actividades y su frecuencia observada se conocen como comportamiento perfilado.

La información rastreada en este panel incluye:

- Organización de ASN: la organización de número de sistema autónomo (ASN) desde la que se realizó la llamada anómala a la API.
- Nombre de usuario: el nombre del usuario que hizo la llamada anómala a la API.
- Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
- Tipo de usuario: el tipo de usuario que hizo la llamada anómala a la API. Los valores posibles son `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.
- Bucket: el nombre del bucket de S3 al que se ha accedido.
- Comportamiento inusual (identidad de usuario): en esta sección se proporcionan detalles adicionales sobre el comportamiento perfilado de la identidad de usuario implicado en el resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de ML de GuardDuty no había visto anteriormente que esta identidad de usuario hiciera esta llamada a la API de esta manera durante el periodo de entrenamiento. Los siguientes detalles adicionales sobre la identidad de usuario están disponibles:
 - Organización de ASN: la organización de ASN desde la que se hizo la llamada anómala a la API.

- **Agente de usuario:** el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
- **Bucket:** el nombre del bucket de S3 al que se ha accedido.
- **Comportamiento inusual (bucket):** en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado del bucket de S3 asociado al resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de ML de GuardDuty no había visto anteriormente que se hicieran llamadas a la API desde este bucket, de esta manera, durante el periodo de entrenamiento. La información rastreada en esta sección incluye:
 - **Organización de ASN:** la organización de ASN desde la que se hizo la llamada anómala a la API.
 - **Nombre de usuario:** el nombre del usuario que hizo la llamada anómala a la API.
 - **Agente de usuario:** el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
 - **Tipo de usuario:** el tipo de usuario que hizo la llamada anómala a la API. Los valores posibles son `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.

 Note

Para más información sobre los comportamientos históricos, seleccione Comportamiento histórico en las secciones Comportamiento inusual (cuenta), ID de usuario o Bucket para ver detalles sobre el comportamiento esperado de su cuenta en cada una de las siguientes categorías: Raro (menos de una vez al mes), Poco frecuente (varias veces al mes) o Frecuente (diario o semanal), según la frecuencia con la que se usen en la cuenta.

- **Comportamiento inusual (base de datos):** en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado de la instancia de base de datos asociada al resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de ML de GuardDuty no había visto anteriormente un intento de inicio de sesión a esta instancia de base de datos, de esta manera, durante el periodo de entrenamiento. La información recopilada en esta sección del panel de resultados incluye:
 - **Nombre de usuario:** el nombre de usuario utilizado para llevar a cabo el intento de inicio de sesión anómalo.

- **Organización de ASN:** la organización de ASN desde la que se hizo el intento de inicio de sesión anómalo.
- **Nombre de la aplicación:** el nombre de la aplicación utilizada para llevar a cabo el intento de inicio de sesión anómalo.
- **Nombre de base de datos:** el nombre de la instancia de base de datos implicada en el intento de inicio de sesión anómalo.

La sección Comportamiento histórico proporciona más contexto sobre los Nombres de usuario, Organizaciones de ASN, Nombres de las aplicaciones y Nombres de bases de datos observados anteriormente para la base de datos asociada. Cada valor único tiene un recuento asociado que representa el número de veces que se observó este valor en un evento de inicio de sesión exitoso.

- **Comportamiento inusual (clúster de Kubernetes de la cuenta, espacio de nombres de Kubernetes y nombre de usuario de Kubernetes):** esta sección proporciona detalles adicionales sobre el comportamiento perfilado para el clúster de Kubernetes y el espacio de nombres asociados al resultado. Cuando un comportamiento no es identificado como histórico, significa que el modelo de ML de GuardDuty no ha observado previamente esta cuenta, clúster, espacio de nombres o nombre de usuario de esta manera. La información recopilada en esta sección del panel de resultados incluye:
 - **Nombre de usuario:** el usuario que llamó a la API de Kubernetes asociada al resultado.
 - **Nombre de usuario suplantado:** el usuario suplantado por `username`.
 - **Espacio de nombres:** el espacio de nombres de Kubernetes dentro del clúster de Amazon EKS en el que se produjo la acción.
 - **Agente de usuario:** el agente de usuario asociado a la llamada a la API de Kubernetes. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `kubectl`.
 - **API:** la API de Kubernetes llamada por `username` dentro del clúster de Amazon EKS.
 - **Información de ASN:** la información de ASN, como la organización y el proveedor de servicios de Internet, asociada a la dirección IP del usuario que realiza esta llamada.
 - **Día de la semana:** el día de la semana en que se realizó la llamada a la API de Kubernetes.
 - **Permiso:** el verbo de Kubernetes y el recurso cuyo acceso se comprueba para indicar si el `username` puede o no utilizar la API de Kubernetes.
 - **Nombre de la cuenta de servicio:** la cuenta de servicio asociada a la carga de trabajo de Kubernetes que proporciona una identidad a la carga de trabajo.
 - **Registro:** el registro del contenedor asociado a la imagen del contenedor que se implementa en la carga de trabajo de Kubernetes.

- **Imagen:** la imagen de contenedor, sin las etiquetas ni el resumen asociados, que se implementa en la carga de trabajo de Kubernetes.
- **Configuración del prefijo de la imagen:** el prefijo de la imagen con la configuración de seguridad del contenedor y la carga de trabajo habilitada, por ejemplo `hostNetwork` o `privileged` para el contenedor que usa la imagen.
- **Nombre del sujeto:** los sujetos, como un `user`, `group`, o `serviceAccountName` que están vinculados a un rol de referencia en un `RoleBinding` o `ClusterRoleBinding`.
- **Nombre del rol:** el nombre del rol que participa en la creación o modificación de roles o en la API `roleBinding`.

Anomalías basadas en el volumen de S3

En esta sección, se detalla la información contextual de las anomalías basadas en el volumen de S3. El resultado basado en el volumen ([Exfiltration:S3/AnomalousBehavior](#)) supervisa un número inusual de llamadas a la API de S3 hechas por los usuarios a los buckets de S3, lo que indica una posible exfiltración de datos. Las siguientes llamadas a la API de S3 se supervisan para detectar anomalías basadas en el volumen.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Las siguientes métricas ayudarían a crear una referencia del comportamiento habitual cuando una entidad de IAM accede a un bucket de S3. Para detectar la exfiltración de datos, el resultado de la detección de anomalías basada en el volumen evalúa todas las actividades con respecto a la referencia de comportamiento habitual. Seleccione Comportamiento histórico en las secciones Comportamiento inusual (identidad de usuario), Volumen observado (identidad de usuario) y Volumen observado (bucket) para ver las siguientes métricas, respectivamente.

- Número de llamadas a la API `s3-api-name` invocadas por el usuario de IAM o rol de IAM (depende de cuál se haya emitido) asociados al bucket de S3 afectado en las últimas 24 horas.
- Número de llamadas a la API `s3-api-name` invocadas por el usuario de IAM o rol de IAM (depende de cuál se haya emitido) asociados a todos los buckets de S3 afectados en las últimas 24 horas.

- Número de llamadas a la API `s3-api-name` en todos los usuarios de IAM o roles de IAM (depende de cuál se haya emitido) asociados al bucket de S3 afectado en las últimas 24 horas.

Anomalías basadas en la actividad de inicio de sesión en RDS

En esta sección, se detalla el recuento de los intentos de inicio de sesión de un actor inusual y se agrupa por el resultado de los intentos de inicio de sesión. [Tipos de resultados de la protección de RDS](#) identifica el comportamiento anómalo mediante la supervisión de los eventos de inicio de sesión para detectar patrones inusuales de `successfulLoginCount`, `failedLoginCount` y `incompleteConnectionCount`.

- `successfulLoginCount`: este contador representa la suma de las conexiones correctas (combinación correcta de atributos de inicio de sesión) hechas a la instancia de base de datos por un actor inusual. Los atributos de inicio de sesión incluyen el nombre de usuario, la contraseña y el nombre de la base de datos.
- `failedLoginCount`: este contador representa la suma de los intentos de inicio de sesión fallidos (incorrectos) hechos para establecer una conexión con la instancia de base de datos. Esto indica que uno o varios atributos de la combinación de inicio de sesión, como el nombre de usuario, la contraseña o el nombre de la base de datos, eran incorrectos.
- `incompleteConnectionCount`: este contador representa el número de intentos de conexión que no se pueden clasificar como exitosos o fallidos. Estas conexiones se cierran antes de que la base de datos proporcione una respuesta. Por ejemplo, se analiza un puerto cuando el puerto de la base de datos está conectado, pero no se envía ningún dato a la base de datos o cuando la conexión se interrumpió antes de que se completara el inicio de sesión en un intento exitoso o fallido.

Agregación de resultados de GuardDuty

GuardDuty actualiza los resultados generados de forma dinámica. Si GuardDuty detecta nueva actividad relacionada con el mismo problema de seguridad, en lugar de crear un resultado nuevo, actualizará el resultado original con los detalles más recientes. Este comportamiento le permite identificar problemas en curso sin necesidad de revisar varios informes similares y reduce el volumen general de los resultados de seguridad que ya conoce.

Por ejemplo, para un resultado `UnauthorizedAccess:EC2/SSHBruteForce`, se agregarán varios intentos de acceso contra la instancia al mismo ID de resultado, lo que aumentará el número de recuento en los detalles del resultado. Esto se debe a que ese resultado representa un único

problema de seguridad con la instancia que indica que el puerto SSH de la instancia no está protegido adecuadamente contra este tipo de actividad. Sin embargo, si GuardDuty detecta actividad de acceso SSH dirigida a una nueva instancia en su entorno, creará un nuevo resultado con un ID de resultado único para alertarle sobre el hecho de que hay un problema de seguridad asociado con el nuevo recurso.

Cuando se agrega un resultado, se actualiza con la información del último caso de esa actividad. Esto significa que, en el ejemplo anterior, si su instancia es el objetivo de un intento de fuerza bruta de un nuevo actor, los detalles del resultado se actualizarán para reflejar la IP remota del origen más reciente y se sustituirá la información más antigua. La información completa sobre los intentos de actividad individuales seguirá estando disponible en los registros de CloudTrail o de flujo de la VPC.

Los criterios que alertan a GuardDuty para que genere un nuevo resultado en lugar de agregar uno existente dependen del tipo de resultado. Nuestros ingenieros de seguridad determinan los criterios de agregación para cada tipo de resultado para proporcionarle la mejor información general de los distintos problemas de seguridad dentro de su cuenta.

Cuando GuardDuty genere un tipo de resultados de secuencia de ataque en su cuenta, el resultado solo se agregará cuando GuardDuty identifique las señales similares en la misma secuencia en su cuenta. De lo contrario, GuardDuty generará otra secuencia de ataque.

Administración de resultados de Amazon GuardDuty

GuardDuty ofrece varias características importantes para ayudarle a clasificar, almacenar y administrar sus resultados. Estas características le ayudarán a adaptar los resultados a su entorno específico, reducir el ruido de los resultados de bajo valor y centrarse en amenazas para su entorno único de AWS. Revise los temas que aparecen en esta página para comprender cómo puede utilizar estas características para aumentar el valor de los resultados de seguridad en el entorno.

Temas:

[Panel de resumen en Amazon GuardDuty](#)

Obtenga información sobre los componentes del panel de resumen disponible en la consola de GuardDuty.

[Filtrado de resultados en GuardDuty](#)

Aprenda a filtrar los resultados de GuardDuty según los criterios que especifique.

[Reglas de supresión en GuardDuty](#)

Obtenga información sobre cómo filtrar automáticamente los resultados de los que GuardDuty le avisa a través de las reglas de supresión. Las reglas de supresión archivan automáticamente los resultados en función de los filtros.

[Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#)

Personalice el alcance de supervisión de GuardDuty mediante listas de IP y de amenazas con base en direcciones IP que son públicamente direccionables. Las listas de IP de confianza evitan que se generen resultados que no sean DNS a partir de IP que considere de confianza, mientras que las listas de Intel de amenazas provocarán que GuardDuty le avise de la actividad de las IP definidas por el usuario.

[Exportar los resultados generados a Amazon S3](#)

Exporte los resultados generados a un bucket de Amazon S3 de forma que pueda mantener registros más allá del periodo de retención de resultados de 90 días en GuardDuty. Utilice estos datos históricos para monitorear posibles actividades sospechosas en la cuenta y evaluar la efectividad de las medidas correctivas implementadas.

Procesamiento de resultados de GuardDuty con Amazon EventBridge

Configure notificaciones automáticas de los resultados de GuardDuty a través de los eventos de Amazon EventBridge. También puede automatizar otras tareas a través de EventBridge para ayudarle a responder a los resultados.

Comprender los registros de CloudWatch y las razones por las que se omiten recursos durante el análisis de Malware Protection for EC2

Descubra cómo puede auditar los registros de CloudWatch para Malware Protection for EC2 de GuardDuty y cuáles son los motivos por los que la instancia de Amazon EC2 o los volúmenes de Amazon EBS impactados pueden haberse omitido durante el proceso de análisis.

Reportar falsos positivos en la protección contra malware para EC2

Obtenga información sobre cómo informar de posibles falsos positivos en detecciones de amenazas en la protección contra malware para S3.

Reportar el producto del análisis de objetos de S3 como falso positivo en la protección contra malware para S3

Obtenga información sobre cómo informar de posibles falsos positivos en detecciones de amenazas en la protección contra malware para S3.

Panel de resumen en Amazon GuardDuty

En el panel Resumen de GuardDuty se proporciona una vista agregada de los resultados de GuardDuty generados en su Cuenta de AWS en la Región de AWS actual.

Si utiliza una cuenta de administrador de GuardDuty, el panel muestra estadísticas y datos agregados de su cuenta y de las cuentas de miembros de la organización.

Visualización del panel Resumen

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

GuardDuty muestra el panel Resumen de forma predeterminada al abrir la consola.

2. En la página Resumen, seleccione la Región de AWS que desee en el selector de regiones en la esquina superior derecha de la consola.
3. En el menú selector de intervalos de fechas, elija el intervalo de fechas del que desee ver el resumen. De forma predeterminada, el panel muestra los datos del día actual, Hoy.

 Note

Si no se generaron resultados durante el intervalo de fechas seleccionado, el panel no tendrá ningún dato que mostrar. Puede actualizar el panel o ajustar el intervalo de fechas.

Temas

- [Descripción general](#)
- [Resultados](#)
- [Tipos de resultados más comunes](#)
- [Resultados por gravedad](#)
- [Cuentas con la mayoría de los resultados](#)
- [Recursos con resultados](#)
- [Resultados menos frecuentes](#)
- [Cobertura de los planes de protección](#)

Descripción general

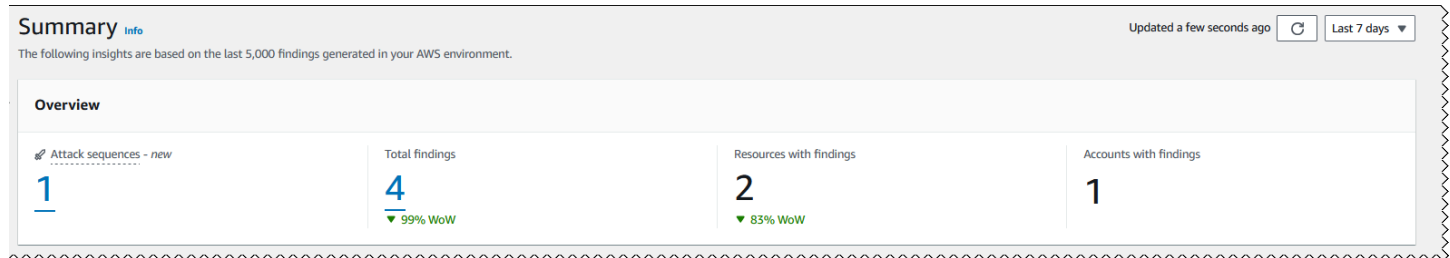
En esta sección se proporcionan los siguientes datos:

- **Secuencias de ataque:** indica el número de resultados de secuencias de ataque que GuardDuty ha generado en su cuenta de la región actual.

GuardDuty detecta posibles ataques en varias etapas en su cuenta. Puede seleccionar el número en Secuencias de ataque para ver sus detalles en la página Resultados.

- **Resultados totales:** indica el número total de resultados generados en su cuenta en la región actual. Esto incluye tanto los resultados individuales como los resultados de la secuencia de ataque.
- **Recursos con resultados:** indica el número de recursos que están asociados a un resultado y que están potencialmente en peligro.
- **Cuentas con resultados:** indica el número de cuentas en las que se generó al menos un resultado. Si es una cuenta independiente, el valor de este campo es 1.

En el caso de los intervalos de tiempo 7 últimos días y 30 últimos días, en el panel Información general se puede mostrar la diferencia porcentual entre los resultados generados semana tras semana (WoW) o mes tras mes (MoM), respectivamente. Si no se generó ningún resultado la semana o el mes anterior y no hay datos para comparar, es posible que la diferencia porcentual no esté disponible.



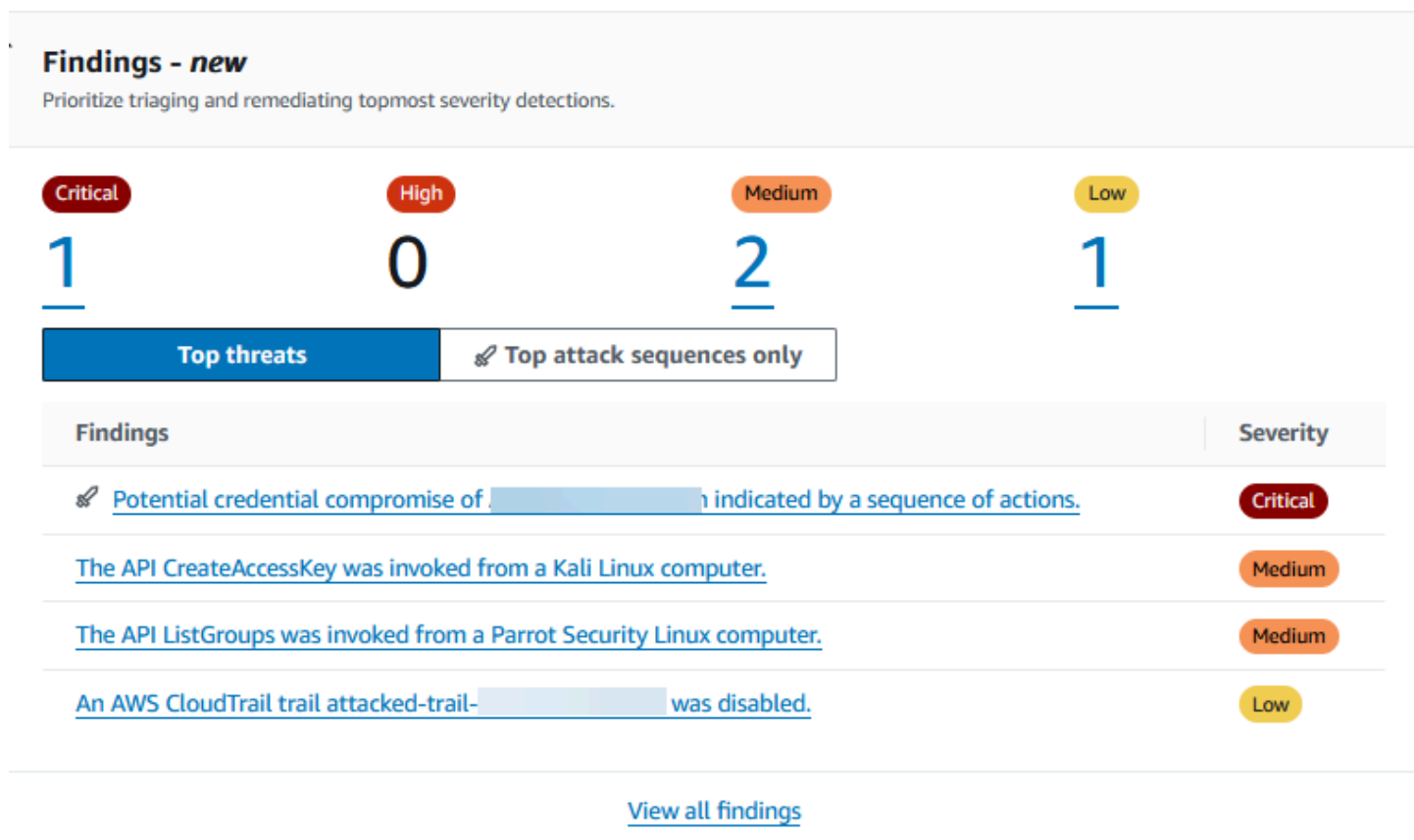
Si se trata de una cuenta de administrador de GuardDuty, todos estos campos proporcionan los datos resumidos de todas las cuentas de miembro de la organización.

Resultados

El widget Resultados muestra hasta ocho resultados principales. Estos resultados se enumeran en función de su nivel de gravedad, y los resultados críticos se muestran primero.

De forma predeterminada, puede ver todos los resultados. Para ver solo los datos de los resultados de las secuencias de ataque, active Solo las secuencias de ataque principales.

En esta lista, puede seleccionar cualquier resultado para ver sus detalles.



Tipos de resultados más comunes

En esta sección se muestra un gráfico circular de los cinco tipos de resultados más comunes generados en la región actual. Al pasar el cursor sobre cada sector del gráfico circular, puede observar lo siguiente:

- Recuento de resultados: indica el número de veces que se ha generado este resultado en el intervalo de tiempo elegido.
- Gravedad: indica el nivel de gravedad del resultado.
- Porcentaje: indica la proporción de este tipo de resultado en relación con el total.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se detectó este tipo de resultado por última vez.

Resultados por gravedad

En esta sección se muestra un gráfico de barras que muestra el número total de resultados en el intervalo de fechas seleccionado. El gráfico desglosa los resultados por gravedad (crítica, alta, media y baja) y le ayuda a ver el número de resultados en fechas específicas dentro del rango.

Para ver los recuentos de cada nivel de gravedad en una fecha específica, coloque el cursor sobre la barra correspondiente del gráfico.

Cuentas con la mayoría de los resultados

En esta sección se proporcionan los siguientes datos:

- **Cuenta:** indica el ID de la Cuenta de AWS en la que se generó el resultado.
- **Recuento de resultados:** indica el número de veces que se generó un resultado para este ID de cuenta.
- **Generado más recientemente:** indica cuánto tiempo ha pasado desde que se generó un tipo de resultado por última vez para este ID de cuenta.
- **Filtro de gravedad:** de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Las opciones posibles para este campo son Todas las gravedades, Gravedad crítica, Gravedad alta y Gravedad media.

Recursos con resultados

En esta sección se proporcionan los siguientes datos:

- **Recurso:** muestra el tipo de recurso potencialmente afectado y, si este recurso pertenece a su cuenta, puede acceder al enlace rápido para ver los detalles del recurso. Si se trata de una cuenta de administrador de GuardDuty, podrá ver los detalles del recurso potencialmente afectado. Para ello, acceda a la consola de GuardDuty con las credenciales de la cuenta de miembro.
- **Cuenta:** indica el ID de la Cuenta de AWS a la que pertenece este recurso.
- **Recuento de resultados:** indica el número de veces que este recurso se asoció a un resultado.
- **Generado más recientemente:** indica cuánto tiempo ha pasado desde que se generó por última vez un tipo de resultado asociado a este recurso.
- **Filtro de tipos de recursos:** de forma predeterminada, los datos se muestran para todos los tipos de recursos. Al usar este filtro, puede elegir ver los datos de un tipo de recurso específico, como Instance, AccessKey o Lambda, entre otros.

- **Filtro de gravedad:** de forma predeterminada, los datos se muestran para todos los niveles de gravedad. Al usar este filtro, puede elegir ver los datos de otros niveles de gravedad. Las opciones posibles son Gravedad crítica, Gravedad alta, Gravedad media y Todos los niveles de gravedad.

Resultados menos frecuentes

En esta sección, se destacan los tipos de búsqueda que se producen con poca frecuencia en su entorno de AWS. Este widget está diseñado para ayudarle a identificar e investigar posibles patrones de amenazas emergentes.

El widget muestra los siguientes datos:

- **Tipo de resultado:** muestra el nombre del tipo de resultado.
- **Recuento de resultados:** indica el número de veces que se generó este tipo de resultado en el intervalo de tiempo elegido.
- **Generado más recientemente:** indica cuánto tiempo ha pasado desde que se generó este tipo de resultado por última vez.
- **Filtro de gravedad:** de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Las opciones posibles para este campo son Gravedad crítica, Gravedad alta, Gravedad media y Todas las gravedades.

Cobertura de los planes de protección

En esta sección se muestran las estadísticas de las cuentas de miembro de su organización. Muestra el número de cuentas de miembro que han habilitado GuardDuty (detección de amenazas fundamentales) en la región actual. Solamente un administrador delegado de GuardDuty puede ver las estadísticas de las cuentas de miembro dentro de su organización. Al crear una nueva organización de AWS, es posible que las estadísticas de toda la organización tarden hasta 24 horas en generarse.

Cómo usar este widget

- **Configuración:** si un plan de protección no está configurado, elija Configurar en la columna Acciones.
- **Visualización de las cuentas habilitadas:** coloque el cursor sobre la barra de la columna Cuentas habilitadas para ver cuántas cuentas ha activado cada plan de protección. Para ver más detalles de la cuenta, seleccione la barra verde y elija Ver cuentas.

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

Filtrado de resultados en GuardDuty

Un filtro de resultado le permite ver los resultados que coinciden con los criterios que especifique y filtrar los resultados que no coincidan. Puede crear fácilmente filtros de resultados con la consola de Amazon GuardDuty o puede crearlos con la API [CreateFilter](#) mediante JSON. Consulte las siguientes secciones para entender cómo crear un filtro en la consola. Para utilizar estos filtros con el objetivo de archivar automáticamente los resultados entrantes, consulte [Reglas de supresión en GuardDuty](#).

Cuando cree filtros, tenga en cuenta la siguiente lista:

- GuardDuty no admite comodines como criterios de filtrado.
- Puede especificar un mínimo de un atributo y un máximo de 50 atributos como criterios para un determinado filtro.

- Cuando se utiliza el operador igual que o no es igual que para filtrar por un valor de atributo, como ID de cuenta, se puede especificar un máximo de 50 valores.
- Cada atributo de los criterios de filtro se evalúa como un operador AND. Se evalúan varios valores para el mismo atributo como AND/OR.
- Para obtener más información acerca del número máximo de índices que puede crear en una Cuenta de AWS en cada Región de AWS, consulte [Cuotas de GuardDuty](#).

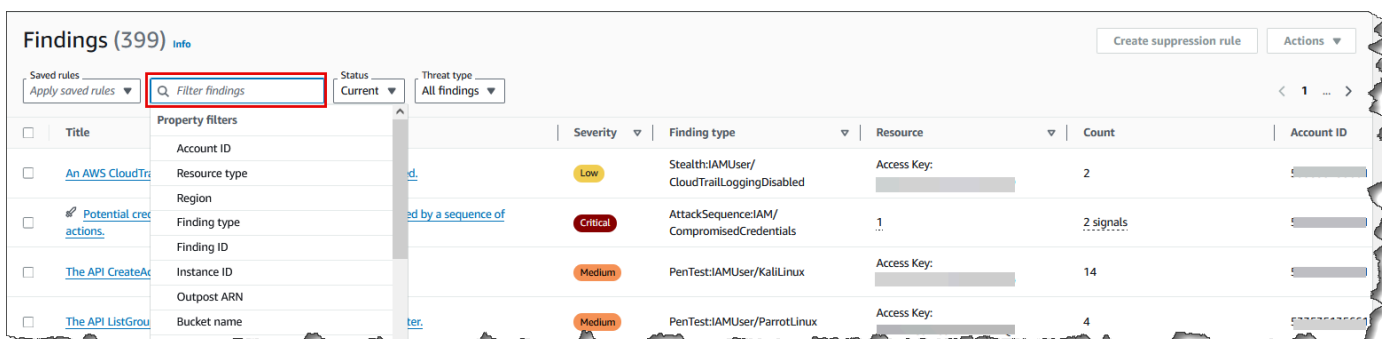
En las siguientes secciones se proporcionan instrucciones sobre cómo crear y guardar filtros mediante la consola GuardDuty y los comandos de API y CLI. Elija su método de acceso preferido para continuar.

Creación y guardado de conjunto de filtros en la consola de GuardDuty

Los filtros de resultados se pueden crear y probar a través de la consola de GuardDuty. Puede guardar los filtros creados a través de la consola para utilizarlos en reglas de supresión o futuras operaciones de filtro. Un filtro se compone de al menos un criterio de filtro, que consiste en un atributo de filtro emparejado con al menos un valor.

Para crear y guardar criterios de filtro (consola)

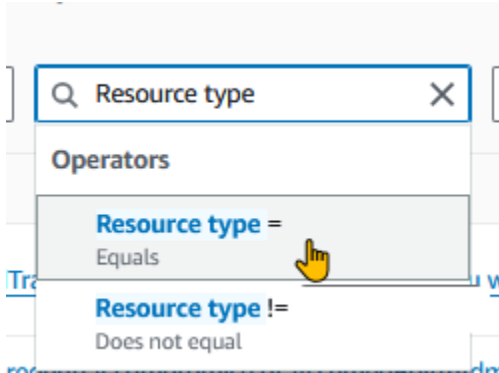
1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación izquierdo, elija Resultados.
3. En la página Resultados, seleccione la barra Filtrar resultados situada junto al menú Reglas guardadas. Aparecerá una lista ampliada de filtros de propiedades.



4. En la lista ampliada de filtros, seleccione un atributo en función del cual desee filtrar la tabla de resultados.

Por ejemplo, para ver los resultados en los que el recurso potencialmente afectado es un S3Bucket, elija el tipo de recurso.

5. En el caso de los operadores, elija uno que ayude a filtrar los resultados para obtener el resultado deseado. Para continuar con el ejemplo del paso anterior, elija Tipo de recurso =. Esto mostrará una lista de tipos de recursos en GuardDuty.



Si su caso de uso requiere excluir resultados específicos, puede elegir el operador no es igual que o !=.

6. Especifique el valor del filtro de propiedades seleccionado. Si es necesario, seleccione Aplicar. Para continuar con el ejemplo del paso anterior, puede elegir S3Bucket.

Esto mostrará los resultados que coinciden con los filtros aplicados.

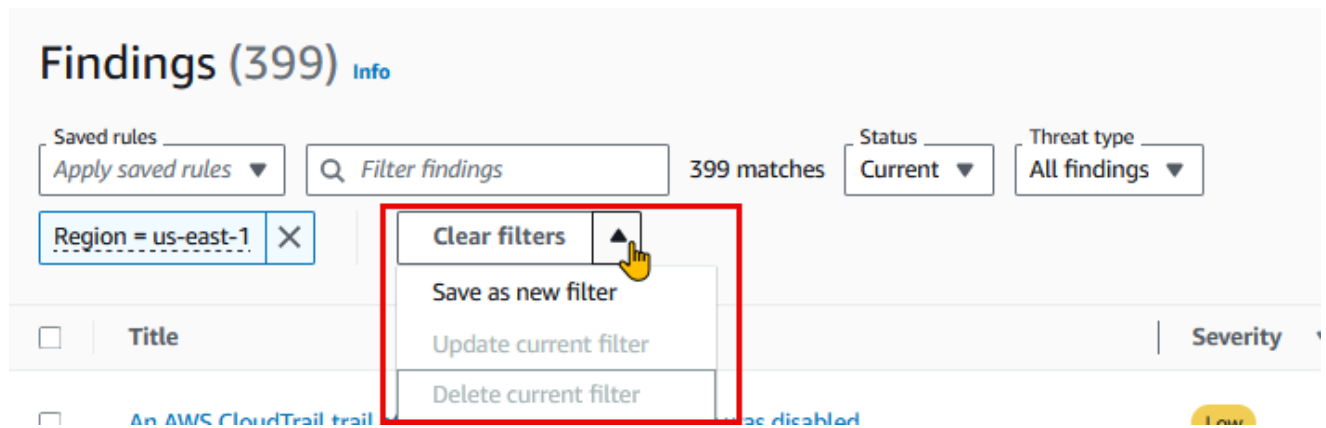
7. Para agregar más de un criterio de filtro, repita los pasos del 3 al 6.

Para obtener una lista completa de los atributos, consulte [Filtros de propiedades en GuardDuty](#).

8. (Opcional) Guardar los atributos y valores especificados como filtros

Para volver a aplicar esta combinación de filtros en el futuro, puede guardar los atributos especificados y sus valores como un conjunto de filtros.

- a. Tras crear un criterio de filtro con uno o más filtros de propiedades, seleccione la flecha en el menú Borrar filtros.



- b. Introduzca el nombre del conjunto de filtros. El nombre debe tener entre 3 y 64 caracteres. Los caracteres válidos son a-z, A-Z, 0-9, punto (.), (guion) (-) y (guion bajo).
- c. La descripción es opcional. Si introduce una descripción, puede tener 512 caracteres como máximo.
- d. Seleccione Crear.

Crear y guardar un conjunto de filtros mediante la API y la CLI de GuardDuty

Puede crear y probar los filtros de resultados mediante comandos de API o CLI. Un filtro se compone de al menos un criterio de filtro, que consiste en un atributo de filtro emparejado con al menos un valor. Puede guardar los filtros para crear [Reglas de supresión](#) o realizar otras operaciones de filtrado más adelante.

Para crear filtros de resultados mediante API/CLI

- Ejecute la API de [CreateFilter](#) con el ID de detector regional de la Cuenta de AWS donde desea crear un filtro.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

- Como alternativa, puede usar la CLI [create-filter](#) para crear y guardar el filtro. Puede utilizar uno o más criterios de filtrado de [Filtros de propiedades en GuardDuty](#).

Utilice los siguientes ejemplos al sustituir los valores de los marcadores de posición que se muestran en rojo.

Ejemplo 1: Cree un filtro nuevo para ver todos los resultados que coincidan con un tipo de resultado específico

En el siguiente ejemplo se crea un filtro que coincide con todos los resultados de PortScan para una instancia creada a partir de una imagen específica. Los valores de los marcadores de posición se muestran en rojo. Sustituya estos valores por valores adecuados para su cuenta. Por ejemplo, sustituya `12abc34d567e8fa901bc2d34EXAMPLE` por su propio ID de detector regional.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},  
"resource.instanceDetails.imageId": {"Equals": ["ami-0a7a207083example"]}} }'
```

Ejemplo 2: cree un filtro nuevo para ver todos los resultados que coincidan con los niveles de gravedad

En el siguiente ejemplo, se crea un filtro que coincide con todos los resultados asociados a los niveles de gravedad HIGH. Los valores de los marcadores de posición se muestran en rojo. Sustituya estos valores por valores adecuados para su cuenta. Por ejemplo, sustituya `12abc34d567e8fa901bc2d34EXAMPLE` por su propio ID de detector regional.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Para API/CLI, [Niveles de gravedad de los resultados](#) se representan como números. Para filtrar los resultados en función de los niveles de gravedad, utilice los siguientes valores:
- Para los niveles de gravedad LOW, utilice { "severity": { "Equals": ["1", "2", "3"] } }
- Para los niveles de gravedad MEDIUM, utilice { "severity": { "Equals": ["4", "5", "6"] } }
- Para los niveles de gravedad HIGH, utilice { "severity": { "Equals": ["7", "8"] } }
- Para los niveles de gravedad CRITICAL, utilice { "severity": { "Equals": ["9", "10"] } }

- Para resultados con varios niveles de gravedad, utilice valores de marcador de posición similares a los del siguiente ejemplo: { "severity": { "Equals": ["7", "8", "9", "10"] } }

En este ejemplo, se mostrarán los resultados que tienen niveles de gravedad HIGH o CRITICAL.

Note

Si se especifica un ejemplo con un solo valor numérico en lugar de todos los valores numéricos asociados a un nivel de gravedad, es posible que la API y la CLI muestren los resultados filtrados. Cuando utilice este conjunto de filtros guardado en la consola de GuardDuty, no funcionará como se esperaba. Esto se debe a que la consola GuardDuty considera los valores del filtro como CRITICAL, HIGH, MEDIUM y LOW. Por ejemplo, se espera que un filtro creado con un comando CLI que incluye { "severity": { "Equals": ["9"] } } muestre un resultado adecuado en API/CLI. Sin embargo, este filtro guardado incluye un nivel de gravedad parcial cuando se usa en la consola GuardDuty y no mostrará el resultado esperado. Esto hace que sea necesario que la API y la CLI especifiquen todos los valores asociados a cada nivel de gravedad.

Filtros de propiedades en GuardDuty

Al crear filtros u ordenar los resultados mediante las operaciones de la API, debe especificar los criterios de filtro en JSON. Estos criterios de filtro se correlacionan con el JSON de los detalles de un resultado. La siguiente tabla contiene una lista de los nombres que se muestran en la consola para los atributos del filtro y sus nombres de campo JSON equivalentes.

Nombre de campo de la consola	Nombre del campo JSON
ID de cuenta	accountId
ID del resultado	id
Región	region
Gravedad	severity

Nombre de campo de la consola	Nombre del campo JSON
	Puede filtrar los tipos de resultados en función de sus niveles de gravedad. Para obtener más información sobre los valores de gravedad, consulte Niveles de gravedad de los resultados de GuardDuty . Si utiliza <code>severity</code> con la API, AWS CLI o CloudFormation, se asigna un valor numérico. Para obtener más información, consulte findingCriteria en la Referencia de la API de Amazon GuardDuty.
Tipo de resultado	tipo
Actualizado a las	updatedAt
ID de clave de acceso	resource.accessKeyDetails.accessKeyId
ID principal	resource.accessKeyDetails.principalId
Nombre de usuario	resource.accessKeyDetails.userName
Tipo de usuario	resource.accessKeyDetails.userType
ID del perfil de instancia de IAM	resource.instanceDetails.iamInstanceProfile.id
ID de instancia	resource.instanceDetails.instanceId
ID de imagen de la instancia	resource.instanceDetails.imageId
Clave de etiqueta de instancia	resource.instanceDetails.tags.key
Valor de etiqueta de instancia	resource.instanceDetails.tags.value
Dirección IPv6	resource.instanceDetails.networkInterfaces.ipv6Addresses
Dirección IPv4 privada	resource.instanceDetails.networkInterfaces.privateIpAddress

Nombre de campo de la consola	Nombre del campo JSON
Nombre DNS público	resource.instanceDetails.networkInterfaces.publicDnsName
IP pública	resource.instanceDetails.networkInterfaces.publicIp
ID de grupo de seguridad	resource.instanceDetails.networkInterfaces.securityGroups.groupId
Nombre del grupo de seguridad	resource.instanceDetails.networkInterfaces.securityGroups.groupName
ID de subred	resource.instanceDetails.networkInterfaces.subnetId
ID de VPC	resource.instanceDetails.networkInterfaces.vpcId
ARN de Outpost	resource.instanceDetails.outpostARN
Tipo de recurso	resource.resourceType
Permisos de bucket	resource.s3BucketDetails.publicAccess.effectivePermission
Nombre del bucket	resource.s3BucketDetails.name
Clave de la etiqueta del bucket	resource.s3BucketDetails.tags.key
valor de la etiqueta del bucket	resource.s3BucketDetails.tags.value
Tipo de bucket	resource.s3BucketDetails.type
Tipo de acción	service.action.actionType
API llamada	service.action.awsApiCallAction.api
Tipo de intermediario de la API	service.action.awsApiCallAction.callerType

Nombre de campo de la consola	Nombre del campo JSON
Código de error de la API	<code>service.action.awsApiCallAction.errorCode</code>
Ciudad del intermediario de la API	<code>service.action.awsApiCallAction.remoteIpDetails.city.cityName</code>
País del intermediario de la API	<code>service.action.awsApiCallAction.remoteIpDetails.country.countryName</code>
Dirección IPv4 del intermediario de la API	<code>service.action.awsApiCallAction.remoteIpDetails.ipAddressV4</code>
Dirección IPv6 de quien realiza la llamada a la API	<code>service.action.awsApiCallAction.remoteIpDetails.ipAddressV6</code>
ID de ASN del intermediario de la API	<code>service.action.awsApiCallAction.remoteIpDetails.organization.asn</code>
Nombre ASN del intermediario de la API	<code>service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg</code>
Nombre del servicio del intermediario de la API	<code>service.action.awsApiCallAction.serviceName</code>
Dominio de la solicitud DNS	<code>service.action.dnsRequestAction.domain</code>
Sufijo de dominio de solicitud de DNS	<code>service.action.dnsRequestAction.domainWithSuffix</code>
Conexión de red bloqueada	<code>service.action.networkConnectionAction.blocked</code>
Dirección de la conexión de red	<code>service.action.networkConnectionAction.connectionDirection</code>
Puerto local de la conexión de red	<code>service.action.networkConnectionAction.localPortDetails.port</code>
Protocolo de conexión de red	<code>service.action.networkConnectionAction.protocol</code>

Nombre de campo de la consola	Nombre del campo JSON
Ciudad de la conexión de red	<code>service.action.networkConnectionAction.remoteIpDetails.city.cityName</code>
País de la conexión de red	<code>service.action.networkConnectionAction.remoteIpDetails.country.countryName</code>
Dirección IPv4 remota de la conexión de red	<code>service.action.networkConnectionAction.remoteIpDetails.ipAddressV4</code>
Dirección IPv6 remota de la conexión de red	<code>service.action.networkConnectionAction.remoteIpDetails.ipAddressV6</code>
ID de ASN de la IP remota de la conexión de red	<code>service.action.networkConnectionAction.remoteIpDetails.organization.asn</code>
Nombre ASN de la IP remota de la conexión de red	<code>service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg</code>
Puerto remoto de la conexión de red	<code>service.action.networkConnectionAction.remotePortDetails.port</code>
Cuenta remota afiliada	<code>service.action.awsApiCallAction.remoteAccountDetails.affiliated</code>
Dirección IPv4 de la persona que llama a la API de Kubernetes	<code>service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV4</code>
Dirección IPv6 de quien realiza la llamada a la API de Kubernetes	<code>service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV6</code>
Espacio de nombres de Kubernetes	<code>service.action.kubernetesApiCallAction.namespace</code>
ID de ASN de quien realiza la llamada a la API de Kubernetes	<code>service.action.kubernetesApiCallAction.remoteIpDetails.organization.asn</code>
URI de solicitud de llamada a la API de Kubernetes	<code>service.action.kubernetesApiCallAction.requestUri</code>

Nombre de campo de la consola	Nombre del campo JSON
Código de estado de la API de Kubernetes	service.action.kubernetesApiCallAction.statusCode
Dirección IPv4 local de conexión de red	service.action.networkConnectionAction.localIpDetails.ipAddressV4
Dirección IPv6 local de la conexión de red	service.action.networkConnectionAction.localIpDetails.ipAddressV6
Protocolo	service.action.networkConnectionAction.protocol
Nombre del servicio de llamada a la API	service.action.awsApiCallAction.serviceName
ID de cuenta de la persona que llama a la API	service.action.awsApiCallAction.remoteAccountDetails.accountId
Nombre de la lista de amenazas	service.additionalInfo.threatListName
Rol de recurso	service.resourceRole
Nombre del clúster de EKS	resource.eksClusterDetails.name
Nombre de la carga de trabajo de Kubernetes	resource.kubernetesDetails.kubernetesWorkloadDetails.name
Nombre de espacio de la carga de trabajo de Kubernetes	resource.kubernetesDetails.kubernetesWorkloadDetails.namespace
Nombre de usuario de Kubernetes	resource.kubernetesDetails.kubernetesUserDetails.username
Imagen del contenedor de Kubernetes	resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image
Prefijo de la imagen del contenedor de Kubernetes	resource.kubernetesDetails.kubernetesWorkloadDetails.containers.imagePrefix

Nombre de campo de la consola	Nombre del campo JSON
ID de análisis	service.ebsVolumeScanDetails.scanId
Nombre de la amenaza de análisis de volúmenes de EBS	service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name
Nombre de la amenaza de análisis de objetos de S3	service.malwareScanDetails.threats.name
Gravedad de la amenaza	service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity
SHA de archivo	service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
Nombre del clúster de ECS	resource.ecsClusterDetails.name
Imagen del contenedor de ECS	resource.ecsClusterDetails.taskDetails.containers.image
ARN de definición de tarea de ECS	resource.ecsClusterDetails.taskDetails.definitionArn
Imagen de contenedor independiente	resource.containerDetails.image
ID de instancia de base de datos	resource.rdsDbInstanceDetails.dbInstanceIdentifier
ID de clúster de base de datos	resource.rdsDbInstanceDetails.dbClusterIdentifier
Motor de base de datos	resource.rdsDbInstanceDetails.engine
Usuario de base de datos	resource.rdsDbUserDetails.user

Nombre de campo de la consola	Nombre del campo JSON
Clave de etiqueta de instancia de base de datos	resource.rdsDbInstanceDetails.tags.key
Valor de etiqueta de instancia de base de datos	resource.rdsDbInstanceDetails.tags.value
SHA-256 ejecutable	service.runtimeDetails.process.executableSha256
Process name	service.runtimeDetails.process.name
Ruta de ejecución	service.runtimeDetails.process.executablePath
Nombre de la función Lambda	resource.lambdaDetails.functionName
ARN de la función Lambda	resource.lambdaDetails.functionArn
Clave de etiqueta de la función de Lambda	resource.lambdaDetails.tags.key
Valor de etiqueta de la función de Lambda	resource.lambdaDetails.tags.value
Dominio de la solicitud DNS	service.action.dnsRequestAction.domainWithSuffix

Reglas de supresión en GuardDuty

Una regla de supresión es un conjunto de criterios, que consta de un atributo de filtro emparejado con un valor, utilizado para filtrar resultados mediante el archivado automático de resultados nuevos que coinciden con los criterios especificados. Las reglas de supresión se pueden utilizar para filtrar los resultados de bajo valor, los resultados positivos falsos o las amenazas sobre las que no se pretende actuar, a fin de facilitar el reconocimiento de las amenazas de seguridad que tienen el mayor impacto en su entorno.

Después de crear una regla de supresión, los nuevos resultados que coincidan con los criterios definidos en la regla se archivan automáticamente siempre que la regla de supresión esté en su lugar. Puede utilizar un filtro existente para crear una regla de supresión o crear una regla de supresión a partir de un nuevo filtro que defina. Puede configurar reglas de supresión para suprimir tipos de hallazgos completos o definir criterios de filtro más detallados para suprimir sólo instancias

específicas de un tipo de hallazgo determinado. Puede editar las reglas de supresión en cualquier momento.

Los resultados suprimidos no se envían a AWS Security Hub CSPM, Amazon Simple Storage Service, Amazon Detective o Amazon EventBridge, lo que reduce el nivel de ruido de resultado si consume los resultados de GuardDuty a través de Security Hub o un SIEM de terceros, así como aplicaciones de alerta y tickets. Si ha activado [Protección contra malware para EC2](#), los resultados suprimidos de GuardDuty no iniciarán un análisis de malware.

GuardDuty continúa generando resultados incluso cuando coinciden con las reglas de supresión; sin embargo, esos resultados se marcan automáticamente como archivados. Los resultados archivados se almacenan en GuardDuty durante 90 días y se pueden consultar en cualquier momento durante ese periodo. Para consultar los resultados suprimidos en la consola de GuardDuty, seleccione Archivado en la tabla de resultados o a través de la API de GuardDuty mediante la API [ListFindings](#) con un criterio `findingCriteria.service.archived` igual a "true".

Note

En un entorno con varias cuentas, solo el administrador de GuardDuty puede crear reglas de supresión.

Uso de reglas de supresión con Detección Extendida de Amenazas

La Detección Extendida de Amenazas GuardDuty detecta automáticamente los ataques en varias etapas que abarcan fuentes de datos, varios tipos de recursos de AWS y tiempo, en una Cuenta de AWS. Correlaciona los eventos en diferentes orígenes de datos para identificar los escenarios que se presentan como una amenaza potencial para su entorno AWS y, a continuación, genera un resultado de la secuencia de ataque. Para obtener más información, consulte [Cómo funciona la Detección Extendida de Amenazas](#).

Al crear reglas de supresión que archivan los resultados, la Detección Extendida de Amenazas no puede usar estos resultados archivados para correlacionar los eventos para las secuencias de ataque. Las normas de supresión amplias podrían afectar a la capacidad de GuardDuty para detectar comportamientos relacionados con la detección de ataques en varias etapas. Los resultados que se archivan debido a las reglas de supresión no se consideran señales para las secuencias de ataque. Por ejemplo, si crea una regla de supresión que archive todos los resultados relacionados con los clústeres de EKS en lugar de centrarse en actividades conocidas específicas, GuardDuty no podrá

usar esos resultados para detectar una secuencia de ataque en la que un actor de amenazas explote un contenedor, obtenga fichas privilegiadas y acceda a recursos confidenciales.

Tenga en cuenta las siguientes recomendaciones de GuardDuty:

- Siga utilizando las reglas de supresión para reducir las alertas procedentes de actividades de confianza conocidas.
- Mantenga las reglas de supresión centradas en comportamientos específicos para los cuales no se desea que GuardDuty genere resultados.

Casos de uso comunes para reglas de supresión y ejemplos

Los siguientes tipos de resultados tienen casos de uso comunes para la aplicación de reglas de supresión. Seleccione el nombre del resultado para obtener más información sobre el mismo. Revise la descripción del caso de uso para decidir si desea crear una regla de supresión para ese tipo de resultado.

Important

GuardDuty recomienda crear reglas de supresión de forma reactiva y únicamente para resultados para los cuales se han identificado repetidamente falsos positivos en el entorno.

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#): utilice una regla de supresión para archivar automáticamente resultados generados cuando se configuran las redes de la VPC para dirigir el tráfico de Internet a fin de que salga desde una puerta de enlace en las instalaciones en lugar de una puerta de enlace de Internet de VPC.

Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de [AWS Outposts](#) o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si el comportamiento es el previsto, se recomienda utilizar reglas de supresión y crear una regla que conste de dos criterios de filtrado. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. El segundo criterio de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR de su puerta de enlace de Internet en las instalaciones. En el siguiente

ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de la dirección IP de la persona que llama a la API.

Finding type: *UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS*
API caller IPv4 address: *198.51.100.6*

 Note

Para incluir varias IP de personas que llaman a la API, puede agregar un nuevo filtro de direcciones IPv4 de las personas que llaman a la API para cada una de ellas.

- [Recon:EC2/Portscan](#): utilice una regla de supresión para archivar automáticamente los resultados cuando utilice una aplicación de evaluación de vulnerabilidades.

La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/Portscan`. El segundo criterio de filtro debe coincidir con la instancia o instancias que alojan estas herramientas de evaluación de vulnerabilidades. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con una determinada AML.

Finding type: *Recon:EC2/Portscan* Instance image ID: *ami-999999999*

- [UnauthorizedAccess:EC2/SSHBruteForce](#): utilice una regla de supresión para archivar automáticamente los resultados cuando tengan como objetivo las instancias de bastión.

Si el objetivo del intento de fuerza bruta es un host bastión, esto podría representar el comportamiento esperado para su entorno de AWS. Si este es el caso, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/SSHBruteForce`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de la instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con un determinado valor de etiqueta de instancia.

Finding type: *UnauthorizedAccess:EC2/SSHBruteForce* Instance tag value: *devops*

- [Recon:EC2/PortProbeUnprotectedPort](#): utilice una regla de supresión para archivar automáticamente los resultados cuando tengan como objetivo las instancias que se hayan visto expuestas de manera intencional.

Puede haber casos en los que las instancias se expongan de forma intencionada, por ejemplo, si están alojando servidores web. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/PortProbeUnprotectedPort`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con una determinada clave de etiqueta de instancia en la consola.

Finding type: *Recon:EC2/PortProbeUnprotectedPort* Instance tag key: *prod*

Reglas de supresión recomendadas para los resultados de la Supervisión en tiempo de ejecución

- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#) se genera cuando un proceso dentro de un contenedor se comunica con el socket de Docker. Es posible que haya contenedores de su entorno que necesiten acceso al socket de Docker por motivos legítimos. El acceso desde dichos contenedores generará resultados `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Si este es el caso de su entorno de AWS, se recomienda que configure una regla de supresión para este tipo de resultado. Los primeros criterios deben utilizar el campo Tipo de resultado con un valor equivalente a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. El segundo criterio de filtro es el campo Ruta ejecutable con un valor igual al `executablePath` del proceso en el resultado generado. De manera alternativa, el segundo criterio de filtro puede utilizar el campo SHA-256 ejecutable con un valor igual al `executableSha256` del proceso en el resultado generado.
- Los clústeres de Kubernetes ejecutan sus propios servidores DNS como pods; por ejemplo, `coredns`. Por lo tanto, para cada búsqueda de DNS desde un pod, GuardDuty captura dos

eventos de DNS: uno del pod y otro del pod del servidor. Esto puede generar duplicados para los siguientes resultados de DNS:

- [Backdoor:Runtime/C&CActivity.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](#)

Los resultados duplicados incluirán los detalles del pod, el contenedor y el proceso que corresponden al pod de su servidor DNS. Puede configurar una regla de supresión para suprimir estos resultados duplicados utilizando estos campos. El primer criterio de filtro debe utilizar el campo Tipo de resultado con un valor igual a un tipo de resultado de DNS de la lista de resultados proporcionada anteriormente en esta sección. El segundo criterio de filtro puede ser Ruta ejecutable con un valor igual al `executablePath` del servidor DNS o SHA-256 ejecutable con un valor igual al `executableSHA256` del servidor DNS en el resultado generado. Como tercer criterio de filtro opcional, puede utilizar el campo Imagen del contenedor de Kubernetes con un valor igual al de la imagen del contenedor del pod del servidor DNS en el resultado generado.

Crear reglas de supresión en GuardDuty

Una regla de supresión es un conjunto de criterios que implica el uso de atributos de filtro y la provisión de valores para los cuales no se desea que GuardDuty genere un tipo de resultado. Los tipos de resultados que cumplen estos criterios se archivan automáticamente. Para reducir el ruido, los resultados suprimidos no se envían a ninguno de los Servicios de AWS con los que se puede integrar. Para obtener más información sobre los casos de uso comunes para la creación de reglas de supresión, consulte [Reglas de supresión](#).

Puede visualizar, crear y administrar reglas de supresión a través de la Consola de GuardDuty. Las reglas de supresión se generan de la misma manera que los filtros y los filtros guardados existentes

se pueden utilizar como reglas de supresión. Para obtener más información acerca de la creación de filtros, consulte [Filtrado de resultados en GuardDuty](#).

Elija el método de acceso que prefiera para crear una regla de supresión para los tipos de resultados de GuardDuty.

Console

Para crear una regla de supresión mediante la consola:

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En la página Resultados, la función Crear una regla de supresión permanece atenuada excepto que añada al menos un criterio de filtrado. Como las reglas de supresión se aplican a los resultados activos y en curso, asegúrese de que el menú de estado esté configurado como Actual.
3. Para añadir uno o más criterios de filtrado, siga los pasos 3 a 7 en [Adding filters on Findings page](#), a continuación, continúe con los pasos siguientes.
4. Una vez que haya agregado los criterios de filtro y haya confirmado que los resultados filtrados cumplen sus requisitos, elija Crear regla de supresión.
5. Introduzca un nombre para la regla de supresión. El nombre debe tener entre 3 y 64 caracteres. Los caracteres válidos son a-z, A-Z, 0-9, punto (.), (guion) (-) y (guion bajo).
6. La descripción es opcional. Si introduce una descripción, puede tener 512 caracteres como máximo.
7. Seleccione Crear.

También puede crear una regla de supresión a partir de un filtro guardado existente. Para obtener más información acerca de la creación de filtros, consulte [Filtrado de resultados en GuardDuty](#).

Para crear una regla de supresión a partir de un filtro guardado:

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En la página Resultados, en el menú Reglas guardadas, seleccione una regla de conjunto de filtros guardada. Esto mostrará automáticamente el conjunto de filtros y los resultados que coincidan con los criterios.
3. También puede agregar más criterios de filtro a esta regla guardada. Puede omitir este paso si no necesita criterios de filtro adicionales.

Para añadir uno o más criterios de filtro adicionales, siga los pasos del 2 al final del procedimiento anterior: [To create a suppression rule using the console](#).

4. Si no necesita añadir criterios de filtro adicionales a la regla guardada, siga los pasos del 4 al final del procedimiento anterior: [To create a suppression rule using the console](#).

API/CLI

Para crear una regla de supresión mediante una API:

1. También puede crear reglas de supresión a través de la API [CreateFilter](#). Para ello, especifique los criterios de filtro en un archivo JSON según el formato del ejemplo que se detalla a continuación. El siguiente ejemplo suprimirá cualquier resultado de baja gravedad no archivado que contenga una solicitud de DNS al dominio `test.example.com`. Para los resultados de gravedad media, la lista de entrada será `["4", "5", "7"]`. Para los resultados de gravedad alta, la lista de entrada será `["6", "7", "8"]`. Para los resultados de gravedad crítica, la lista de entrada será `["9", "10"]`. También puede filtrar en función de cualquier valor de la lista.

En el siguiente ejemplo, se añade un filtro para los resultados de gravedad baja.

```
{
  "Criterion": {
    "service.archived": {
      "Eq": [
        "false"
      ]
    },
    "service.action.dnsRequestAction.domain": {
      "Eq": [
        "test.example.com"
      ]
    },
    "severity": {
      "Eq": [
        "1",
        "2",
        "3"
      ]
    }
  }
}
```

```
}
```

Para obtener una lista de los nombres de campo JSON y su equivalente de consola, consulte [Filtros de propiedades en GuardDuty](#).

Para probar sus criterios de filtro, utilice el mismo criterio de JSON en la API [ListFindings](#) y confirme que se hayan seleccionado los resultados correctos. Para probar sus criterios de filtro, la AWS CLI sigue el ejemplo con su propio detectorId y un archivo .json.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
finding-criteria file://criteria.json
```

2. Cargue el filtro para utilizarlo como regla de supresión con la API [CreateFilter](#) o mediante la CLI de AWS según el ejemplo siguiente con su propio ID de detector, un nombre para la regla de supresión y un archivo .json.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

```
aws guardduty create-filter --action ARCHIVE --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria  
file://criteria.json
```

Puede ver una lista de sus filtros mediante programación con la API [ListFilter](#). Para ver los detalles de un filtro individual, proporcione el nombre del filtro a la API [GetFilter](#). Actualice los filtros mediante la API [UpdateFilter](#) o elimínelos con ayuda de la API [DeleteFilter](#).

Eliminar reglas de supresión en GuardDuty

En esta sección se indican los pasos para eliminar una regla de supresión en la Cuenta de AWS en una Región de AWS específica.

Es posible que desee eliminar una regla de supresión que ya no represente un comportamiento esperado en el entorno. Ya no desea suprimir el tipo de resultado asociado para que GuardDuty pueda generar un tipo de resultado.

Si se trata de una cuenta de miembro, la cuenta de administrador puede realizar esta acción en su nombre. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para eliminar una regla de supresión para los tipos de resultados de GuardDuty.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En la página Resultados, seleccione Suprimir resultados para abrir el panel de reglas de supresión.
3. En el menú desplegable Reglas guardadas, seleccione un filtro guardado.
4. Elija Delete rule (Eliminar regla).

API/CLI

Ejecute la API [DeleteFilter](#). Especifique el nombre del filtro y el ID del detector asociado para la región en cuestión.

También puede utilizar el siguiente ejemplo de la AWS CLI. Para ello, sustituya los valores formateados en *rojo*:

```
aws guardduty delete-filter --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP

Para supervisar la seguridad del entorno de AWS, Amazon GuardDuty analiza y procesa los registros de flujos de VPC, los registros de eventos de AWS CloudTrail y los registros de DNS. Al habilitar uno o más [planes de protección GuardDuty centrados en casos de uso](#) (excepto [Supervisión en tiempo de ejecución](#)), puede ampliar las capacidades de monitoreo de GuardDuty.

Con las listas, GuardDuty le ayuda a personalizar el alcance de la detección de amenazas en su entorno. Puede configurar GuardDuty para que deje de generar resultados de sus fuentes de confianza y genere resultados de fuentes maliciosas conocidas a partir de sus listas de amenazas. GuardDuty sigue siendo compatible con las listas de direcciones IP antiguas y amplía la compatibilidad a las listas de entidades (recomendado) que pueden contener direcciones IP, dominios o ambos.

Temas

- [Comprender las listas de entidades y listas de direcciones IP](#)
- [Consideraciones importantes sobre las listas de GuardDuty](#)
- [Formatos de las listas](#)
- [Explicación de los estados de las listas](#)
- [Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP](#)
- [Añadir y activar una lista de entidades o una lista de IP](#)
- [Actualización de una lista de entidades o una lista de direcciones IP](#)
- [Desactivar la lista de entidades o la lista de direcciones IP](#)
- [Eliminar la lista de entidades o la lista de direcciones IP](#)

Comprender las listas de entidades y listas de direcciones IP

GuardDuty ofrece dos enfoques de implementación: listas de entidades (recomendado) y listas de IP. Ambos enfoques ayudan a especificar fuentes confiables, que impiden que GuardDuty genere resultados y amenazas conocidas, que GuardDuty utiliza para generar resultados.

Las listas de entidades admiten tanto direcciones IP como nombres de dominio. Utilizan el acceso directo a Amazon Simple Storage Service (Amazon S3) con un único permiso de IAM que no afecta a los límites de tamaño de las políticas de IAM en múltiples regiones.

Las listas de IP solo admiten direcciones IP y utilizan [Rol vinculado al servicio \(SLR\) de GuardDuty](#) (SLR), por lo que es necesario actualizar las políticas de IAM por región, lo que puede afectar a los límites de tamaño de las políticas de IAM.

Las listas de confianza (tanto listas de entidades como listas de direcciones IP) incluyen entradas en las que puede confiar para una comunicación segura con su infraestructura de AWS. GuardDuty no genera resultados para las entradas que figuran en fuentes de confianza. Solo puede agregar una lista de entidades de confianza y una lista de direcciones IP de confianza por Cuenta de AWS y por región.

Las listas de amenazas (tanto listas de entidades como listas de direcciones IP) incluyen entradas que haya identificado como fuentes maliciosas conocidas. Cuando GuardDuty detecta una actividad que involucra a estas fuentes, genera resultados para alertarlo de posibles problemas de seguridad. Puede crear sus propias listas de amenazas o incorporar fuentes de inteligencia de amenazas de terceros. La inteligencia sobre amenazas de terceros puede ofrecer esta lista, que también se puede crear específicamente para su organización. Además de generar resultados debido a una actividad potencialmente sospechosa, GuardDuty también genera resultados en función de una actividad que involucra entradas de las listas de amenazas. En cada momento, puede cargar hasta seis listas de entidades de amenazas y listas de direcciones IP de amenazas por Cuenta de AWS por región.

Note

Para migrar de listas de direcciones IP a listas de entidades, siga [Requisitos previos para las listas de entidades](#), a continuación, añada y active la lista de entidades requerida. Después de esto, puede optar por desactivar o eliminar la lista de direcciones IP correspondiente.

Consideraciones importantes sobre las listas de GuardDuty

Antes de comenzar a trabajar con las listas, lea las siguientes consideraciones:

- Las listas de IP y de entidades se aplican únicamente al tráfico destinado a dominios y direcciones IP enrutables públicamente.
- En una lista de entidades, las entradas se aplican a los resultados de los registros de consultas de DNS de CloudTrail, VPC Flow Logs en Amazon VPC y Route53 Resolver.

En una lista de direcciones IP, las entradas se aplican a los resultados de los registros de consultas de DNS de CloudTrail, VPC Flow Logs en Amazon VPC, pero no a los de Route53 Resolver.

- Si incluye la misma dirección IP o dominio en las listas de confianza y de amenazas, prevalecerá esta entrada de la lista de confianza. GuardDuty no generará un resultado si existe una actividad asociada a esa esta entrada.
- En un entorno con varias cuentas, solo la cuenta de administrador de GuardDuty puede administrar las listas. Esta configuración se aplica automáticamente a las cuentas de miembros. GuardDuty genera resultados basados en la actividad que involucra direcciones IP (y dominios) maliciosas conocidas de las fuentes de amenazas de la cuenta de administrador y no se generan resultados basados en la actividad que involucra direcciones IP (dominios) de las fuentes de confianza de la cuenta de administrador. Para obtener más información, consulte [Múltiples cuentas en Amazon GuardDuty](#).
- Solo se aceptan direcciones IPv4. No se admiten direcciones IPv6.
- Tras activar, desactivar o eliminar una lista de entidades o una lista de direcciones IP, se estima que el proceso se completará en 15 minutos. En algunos casos, este proceso puede tardar hasta 40 minutos en completarse.
- GuardDuty utiliza una lista para detectar amenazas solo cuando el estado de la lista pasa a ser Activo.
- Siempre que añada o actualice una entrada en la ubicación del bucket S3 de la lista, debe volver a activar la lista. Para obtener más información, consulte [Actualización de una lista de entidades o una lista de direcciones IP](#).
- Las listas de entidades y las direcciones IP tienen cuotas diferentes. Para obtener más información, consulte [Cuotas de GuardDuty](#).

Formatos de las listas

GuardDuty acepta varios formatos de archivo para sus listas y listas de entidades, con un máximo de 35 MB por archivo. Cada formato tiene requisitos y capacidades específicos.

Texto sin formato (TXT)

Este formato admite direcciones IP, rangos de CIDR y nombres de dominio. Cada entrada debe aparecer en una línea independiente.

Example Ejemplo de lista de entidades

```
192.0.2.1
192.0.2.0/24
example.com
```

```
example.org
*.example.org
```

Example Ejemplo de lista de direcciones IP

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

Structured Threat Information Expression (STIX)

Este formato admite direcciones IP, bloques de CIDR y nombres de dominio. STIX le permite incluir contexto adicional en su inteligencia de amenazas. GuardDuty procesa las direcciones IP, los rangos de CIDR y los nombres de dominio de los indicadores STIX.

Example Ejemplo de una lista de entidades

```
<?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 Ejemplo de una lista de direcciones 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>

```

CSV de Open Threat Exchange (OTX)TM

Este formato admite direcciones IP individuales, bloques de CIDR y dominios. Este formato de archivo tiene valores separados por comas.

Example Ejemplo de lista de entidades

```

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 Ejemplo de lista de direcciones IP

```

Indicator type, Indicator, Description

```

```
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

CSV de FireEye™ iSIGHT Threat Intelligence

Este formato admite direcciones IP individuales, bloques de CIDR y dominios. En las siguientes listas de ejemplo se utiliza un formato de CSV de FireEye™.

Example Ejemplo de lista de entidades

```
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
```

```
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
```



```
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
```

AlienVault™ Reputation Feed

En la siguiente lista de ejemplo se utiliza el formato AlienVault.

Example Ejemplo de lista de entidades

```
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 Ejemplo de lista de direcciones 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
```

Explicación de los estados de las listas

Al añadir una lista de entidades o una lista de direcciones IP, GuardDuty muestra el estado de esa lista. La columna Estado indica si la lista está en vigor y si es necesario realizar acciones. La lista siguiente describe los valores de estado válidos:

- **Activa:** indica que la lista se está utilizando actualmente para la detección personalizada de amenazas.
- **Inactiva:** indica que la lista no está en uso actualmente. Para que GuardDuty utilice esta lista para detectar amenazas en su entorno, consulte el paso 3: Activar una lista de entidades o una lista de direcciones IP en [Añadir y activar una lista de entidades o una lista de IP](#).
- **Error:** indica que hay un problema con la lista. Pase el cursor sobre el estado para ver los detalles del error.
- **Activación:** indica que GuardDuty ha iniciado el proceso de activación de la lista. Puede seguir con el monitoreo del estado de esta lista. Si no hay ningún error, el estado debería actualizarse a Activo. Mientras el estado siga siendo Activación, no podrá realizar ninguna acción de esta lista. El estado de la lista puede tardar unos minutos en pasar a Activo.
- **Desactivación:** indica que GuardDuty ha iniciado el proceso de desactivación de la lista. Puede seguir con el monitoreo del estado de esta lista. Si no hay ningún error, el estado debería

actualizarse a Inactivo. Mientras el estado siga siendo Desactivación, no podrá realizar ninguna acción de esta lista.

- Eliminar pendientes: indica que la lista está en proceso de eliminarse. Mientras el estado siga siendo Eliminar pendientes, no podrá realizar ninguna acción de esta lista.

Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP

GuardDuty utiliza listas de entidades y listas de direcciones IP para personalizar la detección de amenazas en su entorno de AWS. Las listas de entidades (recomendado) admiten direcciones IP y nombres de dominio, mientras que las listas de direcciones IP solo admiten direcciones IP. Antes de comenzar a crear estas listas, debe agregar los permisos necesarios para el tipo de lista que desea usar.

Requisitos previos para las listas de entidades

Al añadir listas de entidades, GuardDuty lee las listas de confianza y de inteligencia de amenazas de los buckets de S3. El rol que utilice para crear las listas de entidades debe tener el permiso `s3:GetObject` para que los buckets de S3 contengan estas listas.

Note

En un entorno con varias cuentas, solo la cuenta de administrador de GuardDuty puede administrar las listas, lo cual se aplica de manera automática a las cuentas de miembro.

Si aún no tiene el permiso `s3:GetObject` para la ubicación del bucket de S3, utilice la siguiente política de ejemplo y sustituya *amzn-s3-demo-bucket* por la ubicación del bucket de S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
    }
  ]
}
```

```
}  
]  
}
```

Requisitos previos para las listas de direcciones IP

Algunas identidades de IAM requieren permisos especiales para trabajar con listas de IP de confianza y listas de amenazas en GuardDuty. Una identidad con la política administrada [AmazonGuardDutyFullAccess_v2 \(recomendada\)](#) adjunta solo puede cambiar de nombre y desactivar las listas de IP de confianza y las listas de amenazas cargadas.

Para conceder a diferentes identidades acceso completo para trabajar con listas de IP de confianza y listas de amenazas (además de cambiar de nombre y desactivar estas listas, esto incluye la adición, activación, eliminación y actualización de la ubicación o el nombre de las listas), asegúrese de que las siguientes acciones estén presentes en la política de permisos adjunta a un usuario, grupo o rol:

```
{  
  "Effect": "Allow",  
  "Action": [  
    "iam:PutRolePolicy",  
    "iam>DeleteRolePolicy"  
  ],  
  "Resource": "arn:aws:iam::555555555555:role/aws-service-role/  
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"  
}
```

Important

Estas acciones no se incluyen en la política administrada AmazonGuardDutyFullAccess.

Uso del cifrado SSE-KMS con listas de entidades y listas de IP

GuardDuty admite los siguientes cifrado para las listas: SSE-AES256 y SSE-KMS. No se admite SSE-C. Para obtener más información sobre los tipos de cifrado para S3, consulte [Protección de los datos con el cifrado del servidor](#).

Independientemente de si utiliza listas de entidades o listas de IP, si utiliza SSE-KMS, añada la siguiente declaración a su política AWS KMS key. Sustituya **123456789012** por el ID de su propia cuenta.

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

Añadir y activar una lista de entidades o una lista de IP

Las listas de entidades y las listas de direcciones IP le ayudan a personalizar las capacidades de detección de amenazas de GuardDuty. Para obtener más información sobre estas listas, consulte [Comprender las listas de entidades y listas de direcciones IP](#). Para gestionar los datos fiables y de inteligencia de amenazas de su entorno de AWS, GuardDuty recomienda utilizar listas de entidades. Antes de comenzar, consulte [Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP](#).

Elija uno de los siguientes métodos de acceso para agregar y activar una lista de entidades, una lista de entidades de amenazas, una lista de IP de confianza o una lista de IP de amenazas.

Console

(Opcional) Paso 1: obtención de la URL de ubicación de la lista

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3>.
2. En el panel de navegación, elija Buckets.
3. Elija el nombre del bucket de Amazon S3 que contiene la lista específica que desea agregar.
4. Elija el nombre del objeto (lista) para consultar sus detalles.
5. En la pestaña Propiedades, copie el URI de S3 de este objeto.

Paso 2: Añadir datos de inteligencia de amenazas o de confianza

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Listas, seleccione la pestaña Listas de entidades o Listas de direcciones IP.

4. En función de la pestaña seleccionada, elija agregar una lista de confianza o una lista de amenazas.
5. En el cuadro de diálogo para agregar una lista de confianza o una lista de amenazas, haga lo siguiente.
 - a. En Nombre de la lista, ingrese un nombre para la lista.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS y región.

- b. En Ubicación, indique la ubicación en la que ha cargado la lista. Si aún no la tiene, consulte [Step 1: Fetching location URL of your list](#).

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Formato de la URL de ubicación:

- `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. (Opcional) Para el propietario esperado del bucket, puede introducir el ID de Cuenta de AWS propietario del bucket de Amazon S3 especificado en el campo Ubicación.

Si no especificas un propietario de ID de Cuenta de AWS, GuardDuty se comporta de forma diferente para las listas de entidades y las listas de direcciones IP. En el caso de las listas de entidades, GuardDuty validará que la cuenta de miembro actual sea propietaria del bucket de S3 especificado en el campo Ubicación. En el caso de las listas de direcciones IP, si no se especifica un propietario de ID de la Cuenta de AWS, GuardDuty no realiza ninguna validación.

Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un error al activar la lista.

- d. Active la casilla I agree.
- e. Elija Add list. De forma predeterminada, el estado de la lista agregada es Inactivo. Para que la lista sea efectiva, debe activarla.

Paso 3: Activar una lista de entidades o una lista de direcciones IP

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Listas, seleccione la pestaña en la que desee activar la lista: Listas de entidades o Listas de direcciones IP.
4. Seleccione una lista que desea activar. Esto habilitará el menú Acción y Edición.
5. Elija Acción y, a continuación, elija Activar.

API/CLI

Para añadir y activar una lista de entidades de confianza

1. Ejecute [CreateTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
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
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de entidad de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el ID de la Cuenta de AWS asociado a este valor de `--detector-id` sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Para añadir y activar listas de entidades de amenazas

1. Ejecute [CreateThreatEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
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
```


Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de entidad de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el ID de la Cuenta de AWS asociado a este valor de `--detector-id` sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Creación y activación de una lista de direcciones IP de confianza

1. Ejecute [CreateIPSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS y región.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de direcciones IP de confianza.

```
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
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de IP de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no se especifica el ID de la cuenta que posee el bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de cuenta para el parámetro `expected-bucket-owner`, GuardDuty valida que este ID de Cuenta de AWS sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Para añadir y activar listas de IP de amenazas

1. Ejecute [CreateThreatIntelSet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS y región.

2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de amenazas.

```
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
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de IP de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no se especifica el ID de la cuenta que posee el bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de cuenta para el parámetro `expected-bucket-owner`, GuardDuty valida que este ID de Cuenta de AWS sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Después de activar una lista de entidades o de direcciones IP, es posible que la lista tarde unos minutos en surtir efecto. Para obtener más información, consulte [Consideraciones importantes sobre las listas de GuardDuty](#).

Actualización de una lista de entidades o una lista de direcciones IP

Las listas de entidades y las listas de direcciones IP le ayudan a personalizar las capacidades de detección de amenazas de GuardDuty. Para obtener más información sobre estas listas, consulte [Comprender las listas de entidades y listas de direcciones IP](#).

Puede actualizar el nombre de una lista, la ubicación del bucket en S3, el identificador de cuenta del propietario previsto del bucket y las entradas de una lista existente. Si actualiza las entradas en una lista, debe seguir los pasos para activar la lista de nuevo para que GuardDuty utilice la versión más reciente de la lista. Es posible que, después de actualizar o activar una lista de entidades o de direcciones IP, se necesiten unos minutos para que se encuentre efectiva. Para obtener más información, consulte [Consideraciones importantes sobre las listas de GuardDuty](#).

 Note

Si el estado de una lista es Activación, Desactivación o Eliminación de datos pendientes, debe esperar unos minutos antes de realizar cualquier acción. Para obtener información sobre estos estados, consulte [Explicación de los estados de las listas](#).

Elija uno de los métodos de acceso de la para actualizar una lista de entidades o de direcciones IP.

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Listas, seleccione la pestaña correspondiente: Listas de entidades o Listas de direcciones IP.
4. Seleccione una lista (de confianza o de amenazas) que desee actualizar. Esto habilitará el menú Acción y Edición.
5. Seleccione Editar.
6. En el cuadro de diálogo para actualizar la lista, especifique los detalles que desee actualizar.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS y región.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

7. (Opcional) Para el propietario esperado del bucket, puede introducir el ID de Cuenta de AWS propietario del bucket de Amazon S3 especificado en el campo Ubicación.

Si no especificas un propietario de ID de Cuenta de AWS, GuardDuty se comporta de forma diferente para las listas de entidades y las listas de direcciones IP. En el caso de las listas de entidades, GuardDuty validará que la cuenta de miembro actual sea propietaria del bucket de S3 especificado en el campo Ubicación. En el caso de las listas de direcciones IP, si

no se especifica un propietario de ID de la Cuenta de AWS, GuardDuty no realiza ninguna validación.

Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un error al activar la lista.

8. Seleccione la casilla Estoy de acuerdo y, a continuación, elija Actualizar lista.

API/CLI

Para empezar con los siguientes procedimientos, necesitará el identificador, como `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` o `threatIpSet`, que esté asociado al recurso de lista que desee actualizar.

Para actualizar y activar una lista de entidades de confianza

1. Ejecute [UpdateTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidad de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

2. Como alternativa, puede ejecutar el siguiente comando AWS Command Line Interface que actualizará el name de la lista de la y también la activará:

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de entidad de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el ID de la Cuenta de AWS asociado a este valor de `--detector-id` sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Para actualizar y activar una lista de entidades de amenazas

1. Ejecute [UpdateThreatEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

2. Como alternativa, puede ejecutar el siguiente comando AWS Command Line Interface que actualizará el name de la lista de la y también la activará:

```
aws guardduty update-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--threat-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de entidad de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`

El parámetro `expected-bucket-owner` es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el ID de la Cuenta de

AWS asociado a este valor de `--detector-id` sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Para actualizar y activar una lista de direcciones IP de confianza

1. Ejecute [CreateIPSet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS y región.

2. También puede ejecutar el siguiente comando AWS Command Line Interface que también activa la lista.

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no se especifica el ID de la cuenta que posee el bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID

de cuenta para el parámetro `expected-bucket-owner`, GuardDuty valida que este ID de Cuenta de AWS sea propietario del bucket S3 especificado en el parámetro `--location`. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Para añadir y activar listas de IP de amenazas

1. Ejecute [CreateThreatIntelSet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS y región.

2. También puede ejecutar el siguiente comando AWS Command Line Interface que también activa la lista.

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no se especifica el ID de la cuenta que posee el bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de cuenta para el parámetro `expected-bucket-owner`, GuardDuty valida que este ID de Cuenta de AWS sea propietario del bucket S3 especificado en el parámetro `--location`.

Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Desactivar la lista de entidades o la lista de direcciones IP

Si ya no desea que GuardDuty utilice una lista, puede desactivarla. El proceso puede tardar unos minutos en completarse. Para obtener más información, consulte [Consideraciones importantes sobre las listas de GuardDuty](#). Una vez desactivada la lista, las entradas de la lista de entidades o de la lista de direcciones IP no afectarán a la detección de amenazas en GuardDuty.

Elija uno de los métodos de acceso para desactivar la lista.

Console

Para desactivar la lista de entidades o la lista de direcciones IP

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Lista, seleccione la pestaña en la que desee desactivar la lista: Listas de entidades o Lista de direcciones IP.
4. En la pestaña seleccionada, elija la lista que desee desactivar.
5. Elija Acciones y, a continuación, elija Desactivar.
6. Confirme la acción y elija Desactivar.

API/CLI

Para empezar con los siguientes procedimientos, necesitará el identificador, por ejemplo, `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` o `threatIpSet`, que esté asociado al recurso de la lista que desee desactivar.

Para desactivar una lista de entidades de confianza

1. Ejecute [UpdateTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty update-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que desactivará la lista de entidad de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Para desactivar las listas de entidades de amenazas

1. Ejecute [UpdateThreatEntitySet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea desactivar esta lista de entidades de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).
2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty update-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que creará la lista de entidad de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Para desactivar una lista de direcciones IP de confianza

1. Ejecute [UpdateIPSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de direcciones IP de confianza.

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Para desactivar la lista de IP de amenazas

1. Ejecute [UpdateThreatIntelSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea desactivar esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que desactivará la lista de IP de amenazas.

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Eliminar la lista de entidades o la lista de direcciones IP

Cuando ya no desee mantener una entrada de la lista en su conjunto de entidades o de direcciones IP, puede eliminarla. El proceso puede tardar unos minutos en completarse. Para obtener más información, consulte [Consideraciones importantes sobre las listas de GuardDuty](#).

Si el estado de la lista es Activación o Desactivación, debe esperar unos minutos antes de realizar cualquier acción. Para obtener más información, consulte [Explicación de los estados de las listas](#).

Elija uno de los métodos de acceso para eliminar la lista.

Console

Para eliminar la lista de entidades o la lista de direcciones IP

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Lista, seleccione la pestaña en la que desee eliminar la lista: Listas de entidades o Lista de direcciones IP.
4. En la pestaña seleccionada, elija la lista que desee eliminar.
5. Elija Acciones y, a continuación, elija Eliminar.

El estado de la lista cambiará a Eliminar pendiente. Es posible que se tarde unos minutos en eliminar la lista.

API/CLI

Para empezar con los siguientes procedimientos, necesitará el identificador, por ejemplo, `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` o `threatIpSet`, que esté asociado al recurso de la lista que desee eliminar.

Para eliminar una lista de entidades de confianza

1. Ejecute [DeleteTrusteEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea eliminar esta lista de entidades de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).
2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty delete-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que eliminará la lista de entidad de confianza, y por otros valores de marcador de posición que *se muestren de color rojo*.

Para desactivar las listas de entidades de amenazas

1. Ejecute [DeleteThreatEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea eliminar esta lista de entidades de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).
2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty delete-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que eliminará la lista de entidad de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Para eliminar una lista de direcciones IP de confianza

1. Ejecute [DeleteIPSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir el `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de direcciones IP de confianza.

```
aws guardduty delete-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que eliminará la lista de entidad de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Para eliminar la lista de IP de amenazas

1. Ejecute [DeleteThreatIntelSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que eliminará la lista de IP de amenazas.

```
aws guardduty delete-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example
```

Sustituya `detector-id` por el ID de detector de la cuenta de miembro para la que eliminará la lista de entidad de amenazas, y por otros valores de marcador de posición que *se muestren de color rojo*.

Exportar los resultados de GuardDuty generados a buckets de Amazon S3

GuardDuty retiene los resultados generados por un periodo de 90 días. GuardDuty exporta los resultados activos a Amazon EventBridge (EventBridge). Opcionalmente, puede exportar los resultados generados a un bucket de Amazon Simple Storage Service (Amazon S3). Esto ayudará a realizar un seguimiento de los datos históricos de actividades potencialmente sospechosas en la cuenta y a evaluar si las medidas de corrección recomendadas han tenido éxito.

Todos los nuevos resultados activos generados por GuardDuty se exportan automáticamente dentro de los 5 minutos siguientes a la generación del resultado. Puede establecer la frecuencia con la que se exportan a EventBridge las actualizaciones de los resultados activos. La frecuencia que seleccione se aplica a la exportación de nuevas incidencias de resultados existentes a EventBridge, al bucket de S3 (cuando esté configurado) y a Detective (cuando esté integrado). Para obtener información sobre cómo GuardDuty agrega múltiples incidencias de resultados existentes, consulte [Agregación de resultados de GuardDuty](#).

Al configurar los ajustes para exportar resultados a un bucket de Amazon S3, GuardDuty utiliza AWS Key Management Service (AWS KMS) para cifrar los datos de los resultados en el bucket de S3. Para ello, es necesario agregar permisos al bucket de S3 y a la clave de AWS KMS de modo que GuardDuty pueda utilizarlos para exportar resultados de la cuenta.

Contenido

- [Consideraciones](#)
- [Paso 1: Permisos necesarios para la exportación de resultados](#)
- [Paso 2: Asociar la política a la clave de KMS](#)
- [Paso 3: Asociar la política al bucket de Amazon S3](#)
- [Paso 4: Exportar resultados a un bucket de S3 \(consola\)](#)
- [Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados](#)

Consideraciones

Antes de seguir con los requisitos previos y los pasos para exportar los resultados, considere los siguientes conceptos clave:

- La configuración de exportación es regional: debe configurar las opciones de exportación en cada región donde utilice GuardDuty.
- Exportar resultados a buckets de Amazon S3 en diferentes Regiones de AWS (entre regiones): GuardDuty admite las siguientes configuraciones de exportación:
 - El bucket u objeto de Amazon S3, y la clave de AWS KMS deben pertenecer a la misma Región de AWS.
 - En el caso de los resultados generados en una región comercial, puede optar por exportar esos resultados a un bucket de S3 en cualquier región comercial. Sin embargo, no puede exportar estos resultados a un bucket de S3 en una región de inscripción.
 - En el caso de los resultados generados en una región de inscripción, puede optar por exportarlos a la misma región de inscripción en la que se generaron o a cualquier región comercial. Sin embargo, no puede exportar los resultados de una región de inscripción a otra región de inscripción.
- Permisos para exportar resultados: para configurar los ajustes para exportar resultados activos, el bucket de S3 debe tener permisos que permitan a GuardDuty cargar objetos. También debe tener una clave de AWS KMS que GuardDuty pueda usar para cifrar los resultados.

- Los resultados archivados no se exportan: el comportamiento predeterminado es que no se exportan los resultados archivados, incluidas las nuevas instancias de resultados suprimidos.

Cuando un resultado de GuardDuty se genera como Archivado, tendrá que Desarchivarlo. Esto cambia el estado de filtrar resultado a Activo. GuardDuty exporta las actualizaciones a los resultados existentes no archivados en función de cómo se configure [Paso 5: Frecuencia de exportación de los resultados](#).

- La cuenta de administrador de GuardDuty puede exportar resultados generados en cuentas de miembro asociadas: cuando se configura la exportación de resultados en una cuenta de administrador, todos los resultados de las cuentas de miembro asociadas que se generan en la misma región también se exportarán a la misma ubicación que se configuró para la cuenta de administrador. Para obtener más información, consulte [Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro](#).

Paso 1: Permisos necesarios para la exportación de resultados

Al configurar los ajustes para exportar los resultados, se selecciona un bucket de Amazon S3 en el que almacenar los resultados y una clave de AWS KMS que se utilizará para cifrar los datos. Además de los permisos para las acciones de GuardDuty, también debe tener permisos para las siguientes acciones para configurar correctamente los ajustes para exportar resultados:

- `s3:GetBucketLocation`
- `s3:PutObject`

Si necesita exportar los resultados a un prefijo específico de su bucket de Amazon S3, también debe añadir los siguientes permisos al rol de IAM:

- `s3:GetObject`
- `s3:ListBucket`

Paso 2: Asociar la política a la clave de KMS

GuardDuty cifra los datos de los resultados en el bucket mediante AWS Key Management Service. Para configurar correctamente los ajustes, primero deberá dar permiso a GuardDuty para utilizar una clave de KMS. Para conceder los permisos, [adjunte la política](#) a su clave de KMS.

Cuando se utiliza una clave de KMS de otra cuenta, es necesario aplicar la política de claves. Para ello, inicie sesión en la Cuenta de AWS a la que pertenece la clave. Al configurar los ajustes para exportar los resultados, también necesitará el ARN de la clave de la cuenta a la que pertenece la clave.

Para modificar la política de claves de KMS para que GuardDuty cifre los resultados exportados

1. Abra la consola de AWS KMS en <https://console.aws.amazon.com/kms>.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Seleccione una clave de KMS existente o siga los pasos para [Crear una nueva clave](#) en la Guía para desarrolladores de AWS Key Management Service, que utilizará para cifrar los resultados exportados.

 Note

La Región de AWS de la clave de KMS y del bucket de Amazon S3 debe ser la misma.

Puede utilizar el mismo bucket de S3 y el mismo par de claves de KMS para exportar los resultados de cualquier región aplicable. Para obtener más información, consulte [Consideraciones](#) para exportar los resultados entre regiones.

4. En la sección Key policy (Política de claves), elija Edit (Editar).

Si aparece Cambiar a vista de política, elíjala para mostrar la Política de claves y, a continuación, elija Editar.

5. Copie el siguiente bloque de política en la política de clave de KMS, para conceder a GuardDuty permiso para usar la clave.

```
{
  "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. Para editar la política, sustituya los siguientes valores formateados en **rojo** en el ejemplo de la política:
 1. Sustituya el **ARN de la clave de KMS** por el nombre de recurso de Amazon (ARN) de la clave de KMS. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service.
 2. Sustituya **123456789012** por el ID de Cuenta de AWS que posee la cuenta de GuardDuty que exporta los resultados.
 3. Sustituya **Region2** por la Región de AWS donde se generan los resultados de GuardDuty.
 4. Sustituya **SourceDetectorID** por el detectorID de la cuenta de GuardDuty en la región específica donde se generaron los resultados.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Note

Si utiliza GuardDuty en una región de inscripción, sustituya el valor por el “Servicio” por el punto de conexión regional para esa región. Por ejemplo, si utiliza GuardDuty en la región Medio Oriente (Baréin) (me-south-1), sustituya "Service": "guardduty.amazonaws.com" por "Service": "guardduty.me-south-1.amazonaws.com". Para obtener información sobre los puntos de conexión para cada región de inscripción, consulte [Puntos de conexión y cuotas de GuardDuty](#).

7. Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de la política de la clave de KMS es válida.

Seleccione Save.

8. (Opcional) copie la clave de ARN en un bloc de notas para utilizarla en los pasos posteriores.

Paso 3: Asociar la política al bucket de Amazon S3

Agregue permisos al bucket de Amazon S3 al que exportará resultados para que GuardDuty pueda cargar objetos en este bucket de S3. Independientemente de utilizar un bucket de Amazon S3 que pertenezca a la cuenta del usuario o a una Cuenta de AWS diferente, debe agregar estos permisos.

Si en algún momento decide exportar los resultados a un bucket de S3 diferente, para continuar con la exportación de resultados deberá agregar permisos a ese bucket de S3 y volver a configurar los ajustes de exportación de resultados.

Si aún no dispone de un bucket de Amazon S3 al que desee exportar estos resultados, consulte [Crear un bucket](#) en la Guía del usuario de Amazon S3.

Para asociar permisos a la política del bucket de S3

1. Siga los pasos descritos en [Para crear o editar una política de bucket](#) en la Guía del usuario de Amazon S3, hasta que aparezca la página Editar política de bucket.
2. La política de ejemplo muestra cómo conceder a GuardDuty permiso para exportar resultados al bucket de Amazon S3. Si cambia la ruta después de configurar la exportación de resultados, deberá modificar la política para conceder permiso a la nueva ubicación.

Copie la siguiente política de ejemplo y péguela en el Editor de políticas de bucket.

Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de la política de la clave de KMS es válida.

Política de ejemplo de bucket de S

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. Para editar la política, sustituya los siguientes valores formateados en *rojo* en el ejemplo de la política:
 1. Sustituya el *ARN del bucket de Amazon S3* por el nombre de recurso de Amazon (ARN) del bucket de Amazon S3. Encontrará el ARN del bucket en la página Editar política de bucket de la consola <https://console.aws.amazon.com/s3/>.
 2. Sustituya *123456789012* por el ID de Cuenta de AWS que posee la cuenta de GuardDuty que exporta los resultados.
 3. Sustituya *us-east-2* por la Región de AWS donde se generan los resultados de GuardDuty.

4. Sustituya *SourceDetectorID* por el detectorID de la cuenta de GuardDuty en la región específica donde se generaron los resultados.

Para encontrar el detectorId correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

5. Sustituya la parte *[prefijo opcional]* del valor del marcador de posición *ARN/[prefijo opcional] del bucket de S3* por una ubicación de carpeta opcional a la que desee exportar los resultados. Para obtener más información sobre el uso de prefijos, consulte [Organizar objetos mediante prefijos](#) en la Guía del usuario de Amazon S3.

Al proporcionar una ubicación de carpeta opcional que aún no existe, GuardDuty creará esa ubicación solamente si la cuenta asociada al bucket de S3 es la misma que la cuenta que exporta los resultados. Al exportar resultados a un bucket de S3 que pertenece a otra cuenta, la ubicación de la carpeta ya debe existir.

6. Sustituye el *ARN de la clave de KMS* por el nombre de recurso de Amazon (ARN) de la clave de KMS asociada al cifrado de los resultados exportados al bucket de S3. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service.

Note

Si utiliza GuardDuty en una región de inscripción, sustituya el valor por el "Servicio" por el punto de conexión regional para esa región. Por ejemplo, si utiliza GuardDuty en la región Medio Oriente (Baréin) (me-south-1), sustituya "Service": "guardduty.amazonaws.com" por "Service": "guardduty.me-south-1.amazonaws.com". Para obtener información sobre los puntos de conexión para cada región de inscripción, consulte [Puntos de conexión y cuotas de GuardDuty](#).

4. Seleccione Save.

Paso 4: Exportar resultados a un bucket de S3 (consola)

GuardDuty permite exportar resultados a un bucket existente en otra Cuenta de AWS.

Al elegir un bucket nuevo o existente en su cuenta, puede agregar un prefijo. Al configurar la exportación de resultados, GuardDuty crea una nueva carpeta en el bucket de S3 para sus

resultados. El prefijo se añadirá a la estructura de carpetas predeterminada que creó GuardDuty. Por ejemplo, el formato del prefijo opcional `/AWSLogs/123456789012/GuardDuty/Region`.

La ruta completa del objeto de S3 será `amzn-s3-demo-bucket/prefix-name/UUID.jsonl.gz`. El UUID se genera aleatoriamente y no representa el ID del detector ni el ID del resultado.

 Important

La clave de KMS y el bucket de S3 deben estar en la misma región.

Antes de completar estos pasos, asegúrese de que ha asociado las políticas respectivas a la clave de KMS y al bucket de S3 existente.

Configuración de la opción de exportación de resultados

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Configuración.
3. En la página Configuración, bajo Opciones de exportación de resultados, en Bucket de S3, elija Configurar ahora (o Editar, según sea necesario).
4. En ARN del bucket de S3, ingrese el **bucket ARN**. Para encontrar el ARN del bucket, consulte [Ver las propiedades de un bucket de S3](#) en la Guía del usuario de Amazon S3.
5. En ARN de la clave de KMS, ingrese el **key ARN**. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service.
6. Asociar políticas
 - Siga los pasos para asociar la política del bucket de S3. Para obtener más información, consulte [Paso 3: Asociar la política al bucket de Amazon S3](#).
 - Siga los pasos para asociar la política de clave de KMS. Para obtener más información, consulte [Paso 2: Asociar la política a la clave de KMS](#).
7. Seleccione Save.

Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados

Configure la frecuencia para exportar los resultados activos actualizados según convenga al entorno. De forma predeterminada, los resultados actualizados se exportan cada 6 horas. Esto significa que cualquier dato que se actualice después de la exportación más reciente se incluirá en la siguiente exportación. Si los hallazgos actualizados se exportan cada 6 horas y la exportación se produce a las 12:00, cualquier hallazgo que actualice después de las 12:00 se exportará a las 18:00.

Establecimiento de la frecuencia

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. Seleccione Configuración.
3. En la sección Opciones de exportación de resultados, seleccione Frecuencia de los resultados actualizados. Establece la frecuencia de exportación de los resultados actualizados activos tanto a EventBridge como a Amazon S3. Puede elegir entre las siguientes opciones:
 - Actualizar EventBridge y S3 cada 15 minutos
 - Actualizar EventBridge y S3 cada 1 hora
 - Actualizar EventBridge y S3 cada 6 horas (predeterminado)
4. Seleccione Save changes (Guardar cambios).

Procesamiento de resultados de GuardDuty con Amazon EventBridge

GuardDuty publica (envía) de manera automática los resultados como eventos en Amazon EventBridge (anteriormente Eventos de Amazon CloudWatch), un servicio de bus de eventos sin servidor. EventBridge ofrece una transmisión de datos en tiempo casi real desde aplicaciones y servicios a destinos como temas de Amazon Simple Notification Service (Amazon SNS), funciones AWS Lambda y transmisiones de Amazon Kinesis. Para obtener más información, consulte la [Guía del usuario de Amazon EventBridge](#).

EventBridge permite la supervisión y el procesamiento automatizados de los resultados de GuardDuty mediante la recepción de [eventos](#). EventBridge recibe eventos tanto para los resultados recién generados como para los resultados agregados, donde las apariciones posteriores de un resultado existente se combinan con el original. A cada resultado de GuardDuty se le asigna un ID

de resultado. GuardDuty crea un evento de EventBridge para cada resultado con un ID de resultado único. Para obtener información sobre cómo funciona la agregación en GuardDuty, consulte [Agregación de resultados de GuardDuty](#).

Además de la supervisión y el procesamiento automatizados, el uso de EventBridge permite conservar los datos de sus resultados a más largo plazo. GuardDuty guarda los resultados durante 90 días. Con EventBridge, puede enviar los datos de los resultados a su plataforma de almacenamiento preferida y almacenar los datos durante el tiempo que desee. Para retener los resultados durante más tiempo, GuardDuty apoya [Exportar los resultados generados a Amazon S3](#).

Temas

- [Entender la frecuencia de notificación de EventBridge en GuardDuty](#)
- [Configuración de un tema y un punto de conexión de Amazon SNS \(correo electrónico, Slack y Amazon Chime\)](#)
- [Uso de Amazon EventBridge para los resultados de GuardDuty](#)
- [Creación de una regla de EventBridge para los resultados de GuardDuty](#)
- [Regla de EventBridge para entornos de varias cuentas de GuardDuty](#)

Entender la frecuencia de notificación de EventBridge en GuardDuty

En esta sección se explica con qué frecuencia se reciben notificaciones de resultados a través de EventBridge y cómo actualizar la frecuencia para que se produzcan resultados posteriores.

Notificaciones de resultados recién generados con un identificador de resultado único

GuardDuty envía estas notificaciones casi en tiempo real cuando genera un resultado con un ID de resultado único. La notificación incluye todas las apariciones posteriores de este identificador de resultados durante el proceso de generación de la notificación.

La frecuencia de notificación de los resultados recién generados es casi en tiempo real. De forma predeterminada, no se puede modificar esta frecuencia.

Notificaciones de casos de resultados subsiguientes

GuardDuty le agrega todos los casos subsiguientes de un resultado concreto que se produzcan en intervalos de 6 horas de un solo evento. Solo una cuenta de administrador puede actualizar la frecuencia de notificaciones de EventBridge para que se produzcan resultados posteriores.

Una cuenta de miembro no puede actualizar esta frecuencia para su propia cuenta. Por ejemplo, si la cuenta de administrador delegado de GuardDuty actualiza la frecuencia a una hora, todas las cuentas de miembro también adoptarán esta configuración para notificar las incidencias de resultados posteriores que se envíen a EventBridge. Para obtener más información, consulte [Múltiples cuentas en Amazon GuardDuty](#).

Como cuenta de administrador, puede personalizar la frecuencia predeterminada de las notificaciones sobre las incidencias de resultados posteriores. Los valores posibles son 15 minutos, una hora o seis horas, que es el valor predeterminado. Para obtener información acerca de la configuración de la frecuencia de estas notificaciones, consulte [Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados](#).

Para obtener más información sobre la cuenta de administrador que recibe notificaciones de EventBridge para las cuentas de miembros, consulte [Regla de EventBridge para entornos de varias cuentas](#).

Configuración de un tema y un punto de conexión de Amazon SNS (correo electrónico, Slack y Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) es un servicio totalmente administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores. Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío de mensajes a un tema. Un tema es un punto de acceso lógico y un canal de comunicación que le permite agrupar varios puntos de conexión, como AWS Lambda, como Amazon Simple Queue Service (Amazon SQS), HTTP/S y una dirección de correo electrónico.

Note

Se puede agregar un tema de Amazon SNS a una regla de eventos de EventBridge durante la creación de la regla o después de dicha creación.

Crear un tema de Amazon SNS

Para empezar, antes se debe configurar un tema en Amazon SNS y agregar un punto de conexión. Para crear un tema, siga los pasos indicados en [Paso 1: Crear un tema](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Después de crear el tema, copie

el ARN del tema en el portapeles. Utilizará este ARN del tema para continuar con una de las configuraciones preferidas.

Elija un método preferido para establecer la ubicación donde desea enviar los datos de los resultados de GuardDuty.

Email setup

Para configurar un punto de conexión de correo electrónico

Después de [Create an Amazon SNS topic](#), el siguiente paso es crear una suscripción a este tema. Siga los pasos indicados en [Paso2: Creación de una suscripción a un tema de Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

1. Para el ARN del tema, utilice el ARN del tema creado en el paso [Create an Amazon SNS topic](#). El ARN de tema tiene un aspecto similar al siguiente:

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. En Protocol, seleccione Email.
3. En Punto de conexión, escriba la dirección de correo electrónico donde desee que se reciban las notificaciones de Amazon SNS.

Después de creada la suscripción, tendrá que confirmarla a través del cliente de correo electrónico.

Slack setup

Configuración de un Amazon Q Developer en el cliente de aplicaciones de chat - Slack

Después de [Create an Amazon SNS topic](#), el siguiente paso es configurar el cliente para Slack.

Siga los pasos en [Tutorial: Primeros pasos con Slack](#) en la Guía del administrador de aplicaciones de chat de Amazon Q Developer.

Chime setup

Configuración de un Amazon Q Developer en el cliente de aplicaciones de chat - Chime

Después de [Create an Amazon SNS topic](#), el siguiente paso es configurar Amazon Q Developer para Chime.

Siga los pasos en [Tutorial: Primeros pasos con Amazon Chime](#) en la Guía del administrador de aplicaciones de chat de Amazon Q Developer.

Uso de Amazon EventBridge para los resultados de GuardDuty

Con EventBridge, puede crear reglas para especificar los tipos de eventos que desee monitorear. Estas reglas también especifican los servicios y aplicaciones de destino que pueden realizar acciones automatizadas si se producen estos eventos. Un [destino](#) es un recurso o punto de conexión al que EventBridge envía un evento cuando el evento coincide con el patrón de eventos definido para una regla. Cada evento es un objeto JSON que se adapta al esquema de EventBridge para los eventos de AWS y contiene una representación de JSON de un resultado. Puede personalizar la regla para que envíe solo los eventos que cumplan determinados criterios. Para obtener más información, consulte [tema sobre el esquema de JSON]. Como los datos de los resultados están estructurados como [eventos de EventBridge](#), puede monitorear, procesar y actuar en función de los resultados mediante el uso de otros servicios y herramientas.

Para recibir notificaciones acerca de resultados de GuardDuty basados en eventos, debe crear una regla de EventBridge y un destino para GuardDuty. Esta regla permite a EventBridge enviar notificaciones de resultados generados por GuardDuty al destino especificado en la regla.

Note

EventBridge y CloudWatch Events son el mismo servicio subyacente y la misma API. Sin embargo, EventBridge incluye características adicionales que le ayudan a recibir eventos de aplicaciones de software como servicio (SaaS) y de sus propias aplicaciones. Como el servicio y la API subyacentes son los mismos, el esquema de eventos de los resultados de GuardDuty también es el mismo.

Cómo funcionan los resultados archivados y no archivados en GuardDuty con EventBridge

En el caso de los resultados que se archivan de manera manual, la ocurrencia inicial y todas las posteriores de estos resultados (generados una vez que el archivado haya terminado) se envían a EventBridge en función de una frecuencia de notificación específica. Para obtener más información, consulte [Entender la frecuencia de notificación de EventBridge en GuardDuty](#).

En el caso de los resultados que se archivan de manera automática con [Reglas de supresión](#), la ocurrencia inicial y todas las posteriores de estos resultados (generados una vez que el archivado

haya terminado) no se envían a EventBridge. Puede ver los resultados archivados de manera automática en la consola de GuardDuty.

Esquema de evento

Un [patrón de eventos](#) define los datos que EventBridge utiliza para determinar si se debe enviar el evento al destino. El evento de EventBridge para GuardDuty presenta el siguiente formato:

```
{
  "version": "0",
  "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
  "detail-type": "GuardDuty Finding",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "1970-01-01T00:00:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

El valor de `detail` devuelve los detalles en formato JSON de un solo resultado como objeto, en lugar de devolver toda la sintaxis de la respuesta resultados, que puede respaldar varios resultados dentro de una matriz.

Para obtener una lista completa de todos los parámetros incluidos en `GUARDDUTY_FINDING_JSON_OBJECT`, consulte [GetFindings](#). El parámetro `id` que aparece en la `GUARDDUTY_FINDING_JSON_OBJECT` es el ID de resultado descrito anteriormente.

Creación de una regla de EventBridge para los resultados de GuardDuty

En los siguientes procedimientos se explica cómo utilizar la consola de Amazon EventBridge y [AWS Command Line Interface\(AWS CLI\)](#) para crear una regla de EventBridge para los resultados de GuardDuty. La regla detecta eventos de EventBridge que utilizan el esquema y el patrón de eventos para los resultados de GuardDuty y, a continuación, envía esos eventos a una función de AWS Lambda para su procesamiento.

AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. El código se empaqueta y se carga en AWS Lambda como una función de Lambda. AWS Lambda ejecuta a continuación la función cuando esta se invoca. Una función se puede invocar manualmente, automáticamente en respuesta a eventos o en respuesta a solicitudes de aplicaciones

o servicios. Para obtener más información acerca de cómo crear e invocar funciones de Lambda, consulte la [Guía para desarrolladores de AWS Lambda](#).

Elija el método que prefiera para crear una regla de EventBridge que envíe el resultado de GuardDuty a un destino.

Console

Siga estos pasos para utilizar la consola de Amazon EventBridge para crear una regla que envíe automáticamente todos los eventos de resultados de GuardDuty a una función de Lambda para su procesamiento. La regla usa la configuración predeterminada para las reglas que se ejecutan cuando se reciben eventos específicos. Para obtener más información sobre la configuración de reglas o para aprender a crear una regla que utilice una configuración personalizada, consulte [Creación de reglas que reaccionan a los eventos](#) en la Guía del usuario de Amazon EventBridge.

Antes de crear la regla, cree la función de Lambda que quiere que la regla utilice como destino. Cuando cree la regla, tendrá que especificar esta función como destino. Su destino también puede ser el tema de SNS que creó anteriormente. Para obtener más información, consulte [Configuración de un tema y un punto de conexión de Amazon SNS \(correo electrónico, Slack y Amazon Chime\)](#).

Crear una regla para un evento con la consola

1. Inicie sesión en Consola de administración de AWS y abra la consola de Amazon EventBridge en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, en Buses, elija Reglas.
3. En la sección Reglas, elija Crear regla.
4. En la página Definir detalle de la regla, haga lo siguiente:
 - a. En Nombre, ingrese el nombre de la regla.
 - b. (Opcional) En Descripción, ingrese una breve descripción de la regla de autorización.
 - c. En el caso del Bus de eventos, asegúrese de que esté seleccionada la opción predeterminada y que esté activada la opción Habilitar la regla en el bus de eventos seleccionado.
 - d. En Tipo de regla, elija Regla con un patrón de evento.
 - e. Cuando haya terminado, elija Siguiente.
5. En la página Crear patrón de evento, realice una de las siguientes acciones:

- a. En Origen del evento, elija Eventos de AWS o eventos de socios de EventBridge.
- b. (Opcional) En el caso de un evento de muestra, revise un evento de resultados de muestra para que GuardDuty sepa qué puede contener un evento. Para ello, seleccione AWSEventos. A continuación, en Eventos de muestra, seleccione Resultados de GuardDuty.
- c. Opción 1: usar la forma de patrones, una plantilla que proporciona EventBridge

En la sección Patrón de eventos, realice una de las siguientes acciones:

1. En Método de creación, seleccione Usar forma de patrón.
2. En Origen del evento, elija Servicios de AWS.
3. En Servicio de AWS, elija GuardDuty.
4. En Tipo de evento, elija Resultado de GuardDuty.

Cuando haya terminado, elija Siguiente.

- d. Opción 2: Uso de un patrón de eventos personalizado en JSON

En la sección Patrón de eventos, realice una de las siguientes acciones:

1. En Método de creación, elija Patrón personalizado (editor JSON).
2. En el patrón de eventos, pegue el siguiente JSON personalizado para crear una alerta con los resultados medios, altos y críticos. Para obtener más información, consulte [Niveles de gravedad de los resultados](#).

```
{
  "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  
    ]  
  }  
}
```

Cuando haya terminado, elija Siguiente.

6. Opción A: Seleccionar Servicio de AWS - AWS Lambda como objetivo

En la página Seleccionar destino(s), haga lo siguiente:

- a. Para los tipos de destino, seleccione Servicio de AWS.
- b. En Seleccione destino, elija Función de Lambda. Luego, en Función, elija la función de Lambda a la que quiera enviar los eventos de resultados.
- c. En Configurar version/alias, ingrese la configuración de versión o alias de la función de Lambda de destino.
- d. (Opcional) En Configuración adicional, introduzca una configuración personalizada para especificar qué datos de eventos desea enviar a la función de Lambda. También puede especificar cómo gestionar los eventos que no se envíen correctamente a la función.
- e. Cuando haya terminado, elija Siguiente.

7. Opción B: Selección del tema de SNS como destino

En la página Seleccionar destino(s), haga lo siguiente:

- a. Para los tipos de destino, seleccione Servicio de AWS.
- b. Para Seleccione un destino, elija Tema de SNS. A continuación, en Ubicación de destino, seleccione la opción adecuada en función de la ubicación de destino. En la lista Tema, seleccione el nombre del tema de SNS que creó.
- c. Amplíe Configuración adicional. En Configurar entrada de destino, seleccione Transformador de entrada).
- d. Elija Configurar transformador de entrada.
- e. Copie el siguiente código en el campo Ruta de entrada de la sección Transformador de entrada de destino.

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

- f. Copie el código siguiente y péguelo en el campo Plantilla para dar formato al correo electrónico.

```
"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. En la página Configurar etiquetas, si lo desea, introduzca una o más etiquetas para asignarlas a la regla. A continuación, elija Siguiente.
9. En la página Revisar y crear, revise cada configuración y compruebe que es correcta.

Para cambiar una configuración, elija Editar en la sección que contiene la configuración y, a continuación, escriba la configuración adecuada. También puede usar las pestañas de navegación para ir a la página que contiene una configuración.

10. Cuando termine de verificar la configuración, elija Crear regla.

API

El siguiente procedimiento muestra cómo utilizar comandos de la AWS CLI para crear una regla de EventBridge y un destino para GuardDuty. En concreto, el procedimiento muestra cómo crear una regla que permite a EventBridge enviar eventos de todos los resultados generados por GuardDuty a una función de AWS Lambda como destino para dicha regla.

Note

En el procedimiento anterior, se ha utilizado una función de Lambda como destino de la regla que desencadena EventBridge. También puede configurar otros recursos de AWS como destinos para desencadenar EventBridge. GuardDuty y EventBridge admiten los siguientes tipos de destino: instancias de Amazon EC2, secuencias de Amazon Kinesis, tareas de Amazon ECS, máquinas de estado de AWS Step Functions, el comando `run` y destinos integrados. Para obtener más información, consulte [PutTargets](#) en la Referencia de la API de Amazon EventBridge.

Creación de una regla y un destino

1. Para crear una regla que permita a EventBridge enviar eventos para todos los resultados generados por GuardDuty, ejecute el siguiente comando de la CLI de EventBridge.

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\": [\"aws.guardduty\"]}"
```

Puede seguir personalizando la regla de modo que indique a EventBridge que envíe eventos únicamente a un subconjunto de resultados generados por GuardDuty. Este subconjunto se basa en los atributos de resultado o atributos especificados en la regla. Por ejemplo, utilice el siguiente comando de la CLI para crear una regla que permita a EventBridge enviar eventos únicamente de los resultados de GuardDuty con una gravedad de 5 u 8:

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":  
{\"severity\":[5,8]}}"
```

Para ello, puede utilizar cualquiera de los valores de propiedad que están disponibles en el archivo JSON de los resultados de GuardDuty.

2. Para asociar una función de Lambda como un destino de la regla que ha creado en el paso 1, ejecute el siguiente comando de la CLI de CloudWatch.

```
aws events put-targets --rule your-target-name --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your_function
```

Asegúrese de sustituir *your-target-name* en el comando anterior por la función de Lambda real para los eventos de GuardDuty.

3. Para agregar los permisos necesarios para invocar el destino, ejecute el siguiente comando de la CLI de Lambda.

```
aws lambda add-permission --function-name your-target-name --statement-id 1 --  
action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Asegúrese de sustituir *your_function* en el comando anterior por la función de Lambda real para los eventos de GuardDuty.

Regla de EventBridge para entornos de varias cuentas de GuardDuty

Cuando utilice una cuenta de administrador delegado de GuardDuty, puede ver los eventos generados en las cuentas de miembro y tomar medidas con otras aplicaciones y servicios. Las reglas de EventBridge de su cuenta de administrador se desencadenarán en función de los resultados aplicables de sus cuentas de miembro. Si configura la función de resultados a través de EventBridge en la cuenta de administrador, recibirá notificaciones sobre los resultados tanto de la cuenta como de las cuentas de miembro. Por ejemplo, se puede usar EventBridge para enviar automáticamente tipos específicos de nuevos resultados a una función de Lambda que, a su vez, procesa y envía los datos a su sistema de gestión de incidentes y eventos de seguridad (SIEM).

Puede identificar la cuenta de miembro donde se originó el resultado de GuardDuty con el campo `accountId` de los detalles JSON del resultado. Para crear una regla de eventos personalizada para

cuentas de miembros específicas, cree una nueva regla y use la siguiente plantilla en Patrón de eventos. Sustituya **123456789012** por el accountId de la cuenta de miembro para la que desee activar el evento.

```
{
  "source": [
    "aws.guarddduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

 Note

En este ejemplo, se crea una regla que coincide con todos los resultados del identificador de cuenta especificado. Se pueden incluir varios ID de cuenta separándolos con comas, siguiendo la sintaxis JSON.

Comprender los registros de CloudWatch y las razones por las que se omiten recursos durante el análisis de Malware Protection for EC2

Malware Protection for EC2 de GuardDuty publica los eventos en el grupo de registros de Amazon CloudWatch `/aws/guarddduty/malware-scan-events`. Para cada uno de los eventos relacionados con el análisis de malware, puede supervisar el estado y el resultado del análisis de los recursos afectados. Es posible que se hayan omitido determinados recursos de Amazon EC2 y volúmenes de Amazon EBS durante el análisis de Malware Protection for EC2.

Auditar los registros de CloudWatch en Malware Protection for EC2 de GuardDuty

Hay tres tipos de eventos de análisis admitidos en el grupo de registros de CloudWatch `/aws/guardduty/malware-scan-events`.

Nombre del evento de análisis de Malware Protection for EC2	Explicación
EC2_SCAN_STARTED	Se crea cuando Malware Protection for EC2 de GuardDuty inicia el proceso de análisis de malware, como cuando se prepara para tomar una instantánea de un volumen de EBS.
EC2_SCAN_COMPLETED	Se crea cuando se completa el análisis de Malware Protection for EC2 de GuardDuty para al menos uno de los volúmenes de EBS del recurso impactado. Este evento también incluye el valor de <code>snapshotId</code> que pertenece al volumen de EBS analizado. Una vez finalizado el análisis, el resultado será <code>CLEAN</code> , <code>THREATS_FOUND</code> o <code>NOT_SCANNED</code> .
EC2_SCAN_SKIPPED	Se crea cuando el análisis de Malware Protection for EC2 de GuardDuty omite todos los volúmenes de EBS del recurso impactado. Para identificar el motivo de la omisión, seleccione el evento correspondiente y consulte los detalles. Para obtener más información sobre los motivos de la omisión, consulte Motivos para omitir un recurso durante el análisis de malware a continuación.

Note

Si utiliza una AWS Organizations, los eventos de registro de CloudWatch de las cuentas de miembro en Organizations se publican en el grupo de registro de las cuentas de administrador y de miembro.

Elija el método de acceso que prefiera para ver y consultar los eventos de CloudWatch.

Console

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, en Registros, seleccione Grupos de registros. Elija el grupo de registro /aws/guardduty/malware-scan-events para ver los eventos de análisis de Malware Protection for EC2 de GuardDuty.

Para ejecutar una consulta, elija Información de registros.

Para obtener más información sobre cómo ejecutar una consulta, consulte [Análisis de los datos de registros con Información de registros de Amazon CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.

3. Elija ID de análisis para supervisar los detalles del recurso afectado y los resultados de malware. Por ejemplo, puede ejecutar la siguiente consulta para filtrar los eventos de registro de CloudWatch mediante scanId. Asegúrese de utilizar su propio valor de *scan-id* válido.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- Para trabajar con grupos de registros, consulte [Búsqueda de entradas de registro mediante la AWS CLI](#) en la Guía del usuario de Amazon CloudWatch.

Elija el grupo de registro /aws/guardduty/malware-scan-events para ver los eventos de análisis de Malware Protection for EC2 de GuardDuty.

- Para ver y filtrar los eventos de registro, consulte [GetLogEvents](#) y [FilterLogEvents](#), respectivamente, en la Referencia de la API de Amazon CloudWatch.

Retención de registros de Malware Protection for EC2 de GuardDuty

El periodo de retención de registros predeterminado para el grupo de registros `/aws/guardduty/malware-scan-events` es de 90 días y, una vez transcurrido, los eventos de registro se eliminan automáticamente. Para cambiar la política de retención de registros del grupo de registros de CloudWatch, consulte [Cambiar la retención de datos de registro en Registros de CloudWatch](#) en la Guía del usuario de Amazon CloudWatch o [PutRetentionPolicy](#) en la Referencia de la API de Amazon CloudWatch.

Motivos para omitir un recurso durante el análisis de malware

En los eventos relacionados con el análisis de malware, es posible que se hayan omitido algunos recursos de EC2 y volúmenes de EBS durante el proceso de análisis. En la siguiente tabla se enumeran los motivos por los cuales Malware Protection for EC2 de GuardDuty puede no analizar los recursos. Si procede, siga los pasos propuestos para resolver estos problemas y analice estos recursos la próxima vez que la protección contra malware para EC de GuardDuty inicie un análisis de malware. Los demás problemas se utilizan para informarle sobre el curso de los eventos y no son procesables.

Razones de omisión	Explicación	Pasos propuestos	
RESOURCE_NOT_FOUND	El valor de <code>resourceArn</code> proporcionado para iniciar el análisis de malware bajo demanda no se encontró en su entorno de AWS.	Valide el valor de <code>resourceArn</code> de la carga de trabajo de su instancia o contenedor de Amazon EC2 e inténtelo de nuevo.	
ACCOUNT_INELIGIBLE	El ID de la cuenta de AWS desde el que intentó iniciar un análisis de malware	Compruebe que GuardDuty esté habilitado para esta cuenta de AWS.	

Razones de omisión	Explicación	Pasos propuestos	
	bajo demanda no tiene habilitado GuardDuty.	Al habilitar GuardDuty en una Región de AWS nueva, la sincronización puede tardar hasta 20 minutos.	
UNSUPPORTED_KEY_ENCRYPTION	Malware Protection for EC2 de GuardDuty admite volúmenes tanto cifrados como sin cifrar con una clave administrada por el cliente. No admite el análisis de volúmenes de EBS cifrados con el cifrado de Amazon EBS. Actualmente, existe una diferencia regional por la que no se aplica este motivo de omisión. Para obtener más información sobre estas Regiones de AWS, consulte Disponibilidad de características específicas por región.	Sustituya la clave de cifrado por una clave administrada por el cliente. Para obtener más información sobre los tipos de cifrado que admite GuardDuty, consulte Volúmenes de Amazon EBS compatibles con el análisis de malware.	

Razones de omisión	Explicación	Pasos propuestos	
EXCLUDED_BY_SCAN_SETTINGS	La instancia de EC2 o el volumen de EBS se excluyó durante el análisis de malware. Hay dos posibilidades: la etiqueta se agregó a la lista de inclusión, pero el recurso no está asociado a esta etiqueta, la etiqueta se agregó a la lista de exclusión y el recurso está asociado a esta etiqueta o la etiqueta GuardDuty Excluded está establecida en true para este recurso.	Actualice las opciones de análisis o las etiquetas asociadas a su recurso de Amazon EC2. Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario .	
UNSUPPORTED_VOLUME_SIZE	El volumen es mayor que 2048 GB.	No se puede procesar.	
NO_VOLUME_S_ATTACHED	Malware Protection for EC2 de GuardDuty encontró la instancia en la cuenta, pero no había ningún volumen de EBS asociado a esta instancia para continuar con el análisis.	No se puede procesar.	
UNABLE_TO_SCAN	Se trata de un error de servicio interno.	No se puede procesar.	

Razones de omisión	Explicación	Pasos propuestos	
SNAPSHOT_NOT_FOUND	No se encontraron las instantáneas creadas a partir de los volúmenes de EBS y compartidas con la cuenta de servicio, por lo que Malware Protection for EC2 de GuardDuty no pudo continuar con el análisis.	Compruebe CloudTrail para asegurarse de que las instantáneas no se hayan eliminado de forma intencionada.	
SNAPSHOT_QUOTA_REACHED	Ha alcanzado el volumen máximo permitido de instantáneas para cada región. Esto impide no solo retener, sino también crear nuevas instantáneas.	Puede eliminar las instantáneas antiguas o solicitar un aumento de cuota. Puede ver el límite predeterminado de instantáneas por región y consultar cómo solicitar un aumento de cuota en el apartado Service quotas en la Guía de referencia general de AWS.	

Razones de omisión	Explicación	Pasos propuestos	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Se adjuntaron más de 11 volúmenes de EBS a una instancia de EC2. La protección contra malware para EC2 de GuardDuty analizó los primeros 11 volúmenes de EBS, que se obtuvieron al ordenar <code>deviceName</code> alfabéticamente.	No se puede procesar.	

Razones de omisión	Explicación	Pasos propuestos	
UNSUPPORT ED_PRODUC T_CODE_TYPE	GuardDuty puede escanear la mayoría de las instancias con productCode como marketplace . Es posible que algunas instancias del mercado no sean aptas para el análisis. GuardDuty omitirá esos casos y registrará el motivo como UNSUPPORT ED_PRODUC T_CODE_TYPE . Esta compatibilidad varía en AWS GovCloud (US) y en las regiones de China. Para obtener más información, consulte Disponibilidad de características específicas por región. Para obtener más información, consulte AMI pagadas en la Guía del usuario de Amazon EC2. Para obtener más información sobre productCode , consulte ProductCode	No se puede procesar.	

Razones de omisión	Explicación	Pasos propuestos	
	en la Referencia de la API de Amazon EC2.		

Reportar falsos positivos en la protección contra malware para EC2

Los análisis de protección contra malware para EC2 de GuardDuty pueden identificar un archivo inofensivo en la carga de trabajo de contenedor o instancia de Amazon EC2 como malintencionado o perjudicial. Para mejorar su experiencia con la protección contra malware para EC2 y el servicio GuardDuty, puede notificar los productos falsos positivos si cree que un archivo identificado como malintencionado o perjudicial durante un análisis realmente no contiene malware.

Para reportar un producto de análisis de malware de Amazon EC2 como falso positivo

Para iniciar el proceso, contacte a Soporte. Utilice los siguientes pasos para proporcionar detalles sobre el objeto de S3 analizado:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. Elija Análisis de malware de EC2.
3. Elija un análisis para ver su ID de resultado.
4. Proporcione el ID de resultado. También debe proporcionar el hash SHA-256 del archivo. Esto es necesario para garantizar que la protección contra malware para EC2 de GuardDuty haya recibido el archivo correcto.
5. El equipo de Soporte proporcionará una URL previamente firmada de Amazon Simple Storage Service (Amazon S3) que puede utilizar para cargar el archivo potencialmente malicioso y el hash SHA-256. Para obtener información sobre los pasos que se deben seguir para cargar el objeto analizado, consulte [Cargar objetos con URL previamente firmadas](#) en la Guía del usuario de Amazon S3.
6. Informe al equipo de Soporte una vez que haya cargado correctamente el archivo.

El Soporte acusará recibo del archivo. Los miembros del equipo de servicio de GuardDuty analizarán el envío, y tomarán las medidas apropiadas para mejorar su experiencia con la protección contra malware para EC2 y el servicio de GuardDuty. El equipo de Soporte proporcionará actualizaciones sobre el estado del caso. GuardDuty no mantendrá el objeto de S3 durante más de 30 días.

Reportar el producto del análisis de objetos de S3 como falso positivo en la protección contra malware para S3

Un análisis de protección contra malware para S3 puede identificar un objeto como potencialmente malicioso o dañino. Si cree que el objeto de S3 indicado no contiene malware, reporte este resultado de análisis de malware como falso positivo.

Puede enviar un informe de falso positivo, aunque utilice la protección contra malware para S3 de forma independiente. En este caso, GuardDuty no se diseñó para generar un resultado. Para obtener información sobre cómo verificar el estado del análisis y el estado del producto, consulte [Supervisión de los análisis de objetos de S3](#).

Para reportar un producto de análisis de objetos de S3 como falso positivo

Para iniciar el proceso, contacte a Soporte. Utilice los siguientes pasos para proporcionar detalles sobre el objeto de S3 analizado:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. Según el caso de uso, elija los pasos apropiados:

Using Malware Protection for S3 with GuardDuty

1. En el panel de navegación, seleccione Resultados.
2. En la página Resultados, seleccione el resultado falso positivo para ver sus detalles.
3. Revise los detalles del resultado y proporcione el ID del resultado, la región, el nombre del bucket de S3 protegido y la clave del objeto analizado.

En los detalles Ruta del elemento, proporcione el Hash del objeto. Esto es necesario para garantizar que GuardDuty ha recibido el archivo correcto.

Using Malware Protection for S3 independently

Proporcione el nombre del bucket de S3 protegido, el nombre del objeto analizado y la Región de AWS.

3. El equipo de Soporte proporcionará una URL previamente firmada de Amazon Simple Storage Service (Amazon S3) que puede utilizar para cargar el archivo potencialmente malicioso y el hash. Para obtener información sobre los pasos que se deben seguir para cargar el objeto

analizado, consulte [Cargar objetos con URL previamente firmadas](#) en la Guía del usuario de Amazon S3.

4. Después de cargar el objeto de S3, informe al equipo Soporte.

El Soporte acusará recibo del objeto. Los miembros del equipo de servicio de GuardDuty analizarán el envío, y tomarán las medidas apropiadas para mejorar su experiencia con la protección contra malware para S3 y el servicio de GuardDuty. El equipo de Soporte proporcionará actualizaciones sobre el estado del caso. GuardDuty no mantendrá el objeto de S3 durante más de 30 días.

Corregir los resultados de seguridad detectados en GuardDuty

Amazon GuardDuty genera [resultados](#) que indican posibles hallazgos de seguridad asociados con la detección de amenazas básica de GuardDuty y planes de protección dedicados. En las siguientes secciones, se describen los pasos de corrección recomendados para estos escenarios. Si existen escenarios de corrección alternativos, se describirán en las descripciones de cada tipo de resultado. Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la [Tabla de tipos de resultados activos](#).

Contenido

- [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#)
- [Corregir un bucket de S3 potencialmente comprometido](#)
- [Corregir un objeto de S3 potencialmente malicioso](#)
- [Corregir un clúster de ECS potencialmente comprometido](#)
- [Corregir credenciales de AWS potencialmente comprometidas](#)
- [Corregir un contenedor independiente potencialmente comprometido](#)
- [Corregir los resultados de EKS Protection](#)
- [Corregir los resultados de la Supervisión en tiempo de ejecución](#)
- [Corregir una base de datos potencialmente comprometida](#)
- [Corregir una función de Lambda potencialmente comprometida](#)

Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida

Cuando GuardDuty genera [tipos de resultados que indican recursos de Amazon EC2 potencialmente comprometidos](#), entonces el Recurso será Instancia. Los posibles tipos de resultados podrían ser [Tipos de resultados de EC2](#), [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#) o [Tipos de resultados de la protección contra malware para EC2](#). Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de utilizar [Reglas de supresión](#).

Siga los siguientes pasos para corregir la instancia de Amazon EC2 potencialmente comprometida:

1. Identifique la instancia de Amazon EC2 potencialmente comprometida

Examine la instancia posiblemente comprometida en busca de malware y elimínelo. Puede utilizar [Análisis de malware bajo demanda en GuardDuty](#) para identificar el malware en la instancia de EC2 potencialmente afectada o comprobar [AWS Marketplace](#) para ver si hay productos asociados útiles para identificar y eliminar el malware.

2. Aísle la instancia de Amazon EC2 potencialmente comprometida

Si es posible, siga los siguientes pasos para aislar la instancia potencialmente comprometida:

1. Cree un grupo de seguridad de aislamiento dedicado. Un grupo de seguridad de aislamiento solo debe tener acceso entrante y saliente desde direcciones IP específicas. Asegúrese de que no hay ninguna regla de entrada o salida que permita el tráfico para 0.0.0.0/0 (0-65535).
2. Asocie el grupo de seguridad de aislamiento a esta instancia.
3. Elimine todas las asociaciones de grupos de seguridad distintas del grupo de seguridad de aislamiento recién creado de la instancia potencialmente comprometida.

Note

Las conexiones rastreadas existentes no se terminarán como resultado del cambio de grupo de seguridad. Únicamente el tráfico futuro será bloqueado de forma efectiva por el nuevo grupo de seguridad.

Para obtener información sobre cómo bloquear más tráfico de conexiones existentes sospechosas, consulte [Aplicar NACL basadas en loC de red para impedir más tráfico](#) en el Manual de respuesta a incidentes.

3. Identifique el origen de la actividad sospechosa

Si se detecta malware, con base en el tipo de resultado de su cuenta, identifique y detenga la actividad potencialmente no autorizada en su instancia de EC2. Esto puede requerir acciones como cerrar cualquier puerto abierto, cambiar las políticas de acceso y actualizar las aplicaciones para corregir las vulnerabilidades.

Si no puede identificar y detener la actividad no autorizada en la instancia de EC2 potencialmente comprometida, recomendamos que termine la instancia de EC2 comprometida y la sustituya por una nueva instancia según sea necesario. A continuación se enumeran recursos adicionales para proteger instancias EC2:

- Secciones “Seguridad” y “Redes” en [Prácticas recomendadas de Amazon EC2](#)
- [Grupos de seguridad de Amazon EC2 para instancias de Linux](#)
- [Seguridad en Amazon EC2](#)
- [Sugerencias para proteger la instancia EC2](#).
- [AWS Prácticas recomendadas de seguridad de](#)
- [Guía técnica de respuesta a incidentes de seguridad de AWS](#).

4. Consultar AWS re:Post

Vaya a [AWS re:Post](#) para obtener más ayuda.

5. Envíe una solicitud de asistencia técnica

Si es suscriptor de un paquete Premium Support, puede enviar una solicitud de [asistencia técnica](#).

Corregir un bucket de S3 potencialmente comprometido

Cuando GuardDuty genera [Tipos de resultados de S3 Protection de GuardDuty](#), indica que los buckets de Amazon S3 han sido comprometidos. Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de crear [Reglas de supresión](#). Si este comportamiento no era el previsto, siga estos pasos recomendados para remediar un bucket de Amazon S3 potencialmente comprometido en el entorno de AWS:

1. Identifique el recurso de S3 potencialmente comprometido.

Un resultado de GuardDuty para S3 enumerará el bucket de S3 asociado, su nombre de recurso de Amazon (ARN) y su propietario en los detalles del resultado.

2. Identifique el origen de la actividad sospechosa y la llamada a la API que se utilizó.

La llamada a la API utilizada se mostrará como API en los detalles de resultado. El origen será una entidad principal de IAM (ya sea un rol de IAM, un usuario o una cuenta) y los detalles de identificación figurarán en el resultado. Según el tipo de origen, estará disponible la dirección IP remota o la información del dominio de origen, lo que puede ayudarle a evaluar si el origen fue autorizado. Si el resultado implica credenciales de una instancia de Amazon EC2, también se incluirán los detalles de ese recurso.

3. Determine si el origen de la llamada tenía autorización para acceder al recurso identificado.

Por ejemplo, considere lo siguiente:

- Si un usuario de IAM estuvo involucrado, ¿es posible que sus credenciales hayan sido potencialmente comprometidas? Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).
 - Si se ha invocado una API desde una entidad principal que no tiene antecedentes de haber invocado este tipo de API, ¿este origen necesita permisos de acceso para esta operación? ¿Se pueden restringir aún más los permisos del bucket?
 - Si el acceso se vio desde nombre de usuario ANONYMOUS_PRINCIPAL con el tipo de usuario de la AWSAccount, esto indica que el bucket es público y se ha accedido a él. ¿Este bucket debería ser público? Si no es así, consulte las siguientes recomendaciones de seguridad para encontrar soluciones alternativas al uso compartido de los recursos de S3.
 - Si el acceso se hizo mediante una llamada a PreflightRequest correcta desde el nombre de usuario ANONYMOUS_PRINCIPAL y el tipo de usuario de la AWSAccount, esto indica que el bucket tiene una política de intercambio de recursos entre orígenes (CORS) establecida. ¿Este bucket debería tener una política CORS? Si no es así, asegúrese de que el bucket no sea inadvertidamente público y revise las recomendaciones de seguridad que aparecen a continuación en busca de soluciones alternativas al uso compartido de los recursos de S3. Para más información sobre CORS, consulte [Uso compartido de recursos entre orígenes \(CORS\)](#) en la Guía del usuario de S3.
4. Determine si el bucket de S3 contiene datos confidenciales.

Utilice [Amazon Macie](#) para determinar si el bucket de S3 contiene información confidencial, como información de identificación personal (PII), datos financieros o credenciales. Si la detección automática de datos confidenciales está habilitada para su cuenta de Macie, revise los detalles del bucket de S3 para comprender mejor su contenido. Si esta característica está deshabilitada en su cuenta de Macie, se recomienda que la active para agilizar la evaluación. Como alternativa, puede crear y ejecutar un trabajo de detección de datos confidenciales para inspeccionar los objetos del bucket de S3 en busca de datos confidenciales. Para más información, consulte [Discovering sensitive data with Macie](#).

Si se autorizó el acceso, puede ignorar el resultado. La consola <https://console.aws.amazon.com/guardduty/> le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Si determina que los datos de S3 han sido expuestos o que un tercero no autorizado ha accedido a estos, revise las siguientes recomendaciones de seguridad de S3 para reforzar los permisos y

restringir el acceso. Las soluciones de corrección adecuadas dependerán de las necesidades de su entorno específico.

Recomendaciones basadas en las necesidades específicas de acceso al bucket de S3

La siguiente lista ofrece recomendaciones basadas en las necesidades específicas de acceso a los buckets de Amazon S:

- Para disponer de una forma centralizada de limitar el acceso público a los datos de S3, utilice el bloqueo de acceso público de S3. La configuración de bloqueo de acceso público se puede habilitar para los puntos de acceso, los buckets y las cuentas de AWS mediante cuatro configuraciones diferentes para controlar la granularidad del acceso. Para obtener más información, consulte [Configuración de Block Public Access](#) en la Guía del usuario de Amazon S3.
- Las políticas de acceso de AWS se pueden utilizar para controlar cómo los usuarios de IAM pueden acceder a sus recursos o a sus buckets. Para obtener más información, consulte [Uso de políticas de bucket y de suario](#) en la Guía del usuario de Amazon S3.

Además, puede utilizar puntos de conexión de la nube privada virtual (VPC) con políticas de bucket de S3 para restringir el acceso a puntos de conexión de VPC específicos. Para obtener más información, consulte [Control del acceso desde puntos de enlace de la VPC con políticas de bucket](#) en la Guía del usuario de Amazon S3.

- Para permitir temporalmente el acceso a sus objetos de S3 a entidades de confianza ajenas a su cuenta, puede crear una URL prefirrada a través de S3. Este acceso se crea con las credenciales de su cuenta y, según las credenciales utilizadas, puede durar de 6 horas a 7 días. Para obtener más información, consulte [Uso de URL prefirradas para descarga y carga de objetos](#) en la Guía para usuarios de Amazon S3.
- Para los casos de uso que requieren el uso compartido de objetos de S3 entre distintos orígenes, puede utilizar los puntos de acceso de S3 para crear conjuntos de permisos que restrinjan el acceso únicamente a los que están dentro de su red privada. Para obtener más información, consulte [Administración del acceso a conjuntos de datos con puntos de acceso](#) en la Guía del usuario de Amazon S3.
- Para conceder acceso seguro a sus recursos de S3 a otras cuentas de AWS, puede utilizar una lista de control de acceso (ACL). Para obtener más información, consulte [Descripción general de la lista de control de acceso \(ACL\)](#) en la Guía del usuario de Amazon S3.

Para obtener más información sobre las opciones de seguridad de S3, consulte [Prácticas recomendadas de seguridad para Amazon S3](#), en la Guía del usuario de Amazon S3.

Corregir un objeto de S3 potencialmente malicioso

Cuando GuardDuty genera [Tipo de resultado de la protección contra malware para S3](#), indica que un objeto recién cargado en el bucket de Amazon S3 contiene malware. El tipo de recurso es un objeto de S3.

Utilice los siguientes pasos recomendados para corregir potencialmente el resultado generado:

1. Identifique el objeto de S3 potencialmente malicioso. Para ello, compruebe los S3ObjectDetails asociados al resultado.
2. Aísle el objeto de S3 comprometido. Si había habilitado el etiquetado al habilitar la protección contra malware para S3 para el bucket de Amazon S3 asociado, GuardDuty debe haber asignado una etiqueta de malicioso a este objeto. Utilice el control de acceso basado en etiquetas (TBAC) para restringir el acceso a este objeto de S3. Para obtener más información, consulte [Utilizar el control de acceso basado en etiquetas \(TBAC\)](#).

Como alternativa, si ya no necesita este objeto, también puede optar por eliminarlo o trasladarlo a un bucket de S3 aislado. Para obtener información sobre las consideraciones para eliminar un objeto de S3, consulte [Eliminar objetos](#) en la Guía del usuario de Amazon S3.

Corregir un clúster de ECS potencialmente comprometido

Cuando GuardDuty genera [tipos de resultados que indican recursos de Amazon ECS potencialmente comprometidos](#), entonces el recurso será ECSCluster. Los posibles tipos de resultados podrían ser [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#) o [Tipos de resultados de la protección contra malware para EC2](#). Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de utilizar [Reglas de supresión](#).

Siga estos pasos recomendados para corregir un clúster de Amazon ECS potencialmente comprometido en el entorno de AWS:

1. Identifique el clúster de ECS potencialmente comprometido.

El resultado de la protección contra malware de GuardDuty para EC2 correspondiente a ECS proporciona los detalles del clúster de ECS en el panel de detalles del resultado.

2. Evalúe el origen del malware

Evalúe si el malware detectado estaba en la imagen del contenedor. Si había malware en la imagen, identifique todas las demás tareas que se estén ejecutando con esta imagen. Para obtener información sobre la ejecución de tareas, consulte [ListTasks](#).

3. Aísle las tareas potencialmente comprometidas

Para aislar las tareas afectadas, deniegue todo el tráfico de entrada y salida a la tarea. Una regla de denegar todo el tráfico puede ayudarle a detener un ataque que ya está en curso, al cortar todas las conexiones a la tarea.

Si se autorizó el acceso, puede ignorar el resultado. La consola <https://console.aws.amazon.com/guardduty/> le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Corregir credenciales de AWS potencialmente comprometidas

Cuando GuardDuty genera [Tipos de resultados de IAM](#), indica que las credenciales de AWS han sido atacadas. El tipo de recurso potencialmente comprometido es AccessKey.

Para corregir las credenciales potencialmente comprometidas en el entorno de AWS, siga estos pasos:

1. Identifique la entidad de IAM potencialmente comprometida y la llamada a la API utilizada.

La llamada a la API utilizada se mostrará como API en los detalles de resultado. La entidad de IAM (ya sea un usuario o rol de IAM) y su información de identificación se enumerarán en la sección Recurso de los detalles del resultado. El tipo de entidad de IAM implicada puede determinarse mediante el campo Tipo de usuario, el nombre de la entidad de IAM estará en el campo Nombre de usuario. El tipo de entidad de IAM implicada en el resultado también puede determinarse mediante el ID de clave de acceso utilizado.

Para las claves que empiecen con AKIA:

Este tipo de clave es una credencial administrada por el cliente a largo plazo asociada con un usuario de IAM o Usuario raíz de la cuenta de AWS. Para obtener información sobre la administración de claves de acceso para usuarios de IAM, consulte [Administración de las claves de acceso de los usuarios de IAM](#).

Para las claves que empiecen con ASIA:

Este tipo de clave es una credencial temporal a corto plazo generada por AWS Security Token Service. Estas claves existen solo durante un periodo de tiempo breve y no se pueden consultar ni administrar en la consola de administración de AWS. Los roles de IAM siempre utilizarán credenciales de AWS STS, pero también se pueden generar para usuarios de IAM. Para más información sobre AWS STS, consulte [IAM: Temporary security credentials](#).

Si se utilizó un rol, el campo Nombre de usuario indicará el nombre del rol utilizado. Para determinar cómo se solicitó la clave con AWS CloudTrail, puede examinar el elemento `sessionIssuer` de la entrada de registro de CloudTrail. Para obtener más información, consulte [IAM and AWS STS information in CloudTrail](#).

2. Revise los permisos de la entidad de IAM.

Abra la consola de IAM. Según el tipo de entidad utilizada, seleccione la pestaña Usuarios o Roles, y localice la entidad afectada. Para ello, escriba el nombre identificado en el campo de búsqueda. Utilice las pestañas Permisos y Acceso a Advisor para revisar los permisos efectivos para esa entidad.

3. Determine si las credenciales de entidad de IAM se utilizaron legítimamente.

Póngase en contacto con el usuario de las credenciales para determinar si la actividad fue intencionada.

Por ejemplo, averigüe si el usuario hizo lo siguiente:

- Invocó la operación de la API que se muestra en el resultado de GuardDuty
- Invocó la operación de la API en el momento que se muestra en el resultado de GuardDuty
- Invocó la operación de la API desde la dirección IP que se muestra en el resultado de GuardDuty

Si esta actividad es un uso legítimo de las credenciales de AWS, puede omitir este resultado de GuardDuty. La consola <https://console.aws.amazon.com/guardduty/> le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Si no puede confirmar si esta actividad constituye un uso legítimo, podría ser consecuencia de que la clave de acceso concreta, las credenciales de inicio de sesión del usuario de IAM o, posiblemente, toda la Cuenta de AWS, se encuentren comprometidas. Si sospecha que sus credenciales se han

visto afectadas, revise la información en [My Cuenta de AWS may be compromised](#) para corregir el problema.

Corregir un contenedor independiente potencialmente comprometido

Cuando GuardDuty genera [tipos de resultados que indican contenedores potencialmente comprometidos](#), el tipo de recurso será contenedor. Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de utilizar [Reglas de supresión](#).

Para corregir las credenciales potencialmente comprometidas en el entorno de AWS, siga estos pasos:

1. Aísle el contenedor potencialmente comprometido

Los siguientes pasos ayudarán a identificar la carga de trabajo del contenedor potencialmente malicioso:

- Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
- En la página Resultados, seleccione el resultado correspondiente para ver el panel de resultados.
- En el panel de resultados, en la sección Recurso afectado, puede ver el ID y el Nombre del contenedor.

Aísle este contenedor de otras cargas de trabajo de contenedores.

2. Pause el contenedor

Suspenda todos los procesos de su contenedor.

Para obtener información sobre cómo congelar el contenedor, consulte [Pausar un contenedor](#).

Detener el contenedor.

Si el paso anterior no funciona y el contenedor no se detiene, pare el funcionamiento del contenedor. Si ha activado la característica [Retención de instantáneas](#), GuardDuty retendrá las instantáneas de los volúmenes de EBS que contengan malware.

Para obtener información sobre cómo detener el contenedor, consulte [Detener un contenedor](#).

3. Evalúe la presencia de malware

Evalúe si el malware estaba en la imagen del contenedor.

Si se autorizó el acceso, puede ignorar el resultado. La consola <https://console.aws.amazon.com/guardduty/> le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. La consola de GuardDuty le permite configurar reglas para suprimir por completo los resultados individuales para que no aparezcan más. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Corregir los resultados de EKS Protection

Amazon GuardDuty genera [resultados](#) que indican posibles problemas de seguridad de Kubernetes cuando EKS Protection está habilitada para la cuenta. Para obtener más información, consulte [EKS Protection](#). En las siguientes secciones, se describen los pasos de corrección recomendados para estos escenarios. Las acciones de corrección específicas se describen en la entrada de ese tipo de resultado en concreto. Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la [Tabla de tipos de resultados activos](#).

Si alguno de los tipos de resultados de EKS Protection se generó de forma expectante, puede considerar la posibilidad de agregar [Reglas de supresión en GuardDuty](#) para evitar futuras alertas.

Diferentes tipos de ataques y problemas de configuración pueden desencadenar resultados de EKS Protection de GuardDuty. Esta guía sirve de ayuda para identificar las causas raíces de los resultados de GuardDuty en su clúster y contiene información sobre las directrices de corrección adecuadas. A continuación se indican las principales causas raíces que provocaron los resultados de Kubernetes de GuardDuty:

- [Posibles problemas de configuración](#)
- [Corregir usuarios de Kubernetes potencialmente comprometidos](#)
- [Corregir pods de Kubernetes potencialmente comprometidos](#)
- [Corregir nodos de Kubernetes potencialmente comprometidos](#)
- [Corregir imágenes de contenedores potencialmente comprometidas](#)

Note

Antes de la versión 1.14 de Kubernetes, el grupo `system:unauthenticated` estaba asociado a `system:discovery` y `system:basic-user`, que son ClusterRoles,

de manera predeterminada. Esto puede permitir el acceso no deseado de usuarios anónimos. Las actualizaciones del clúster no revocan estos permisos, lo que significa que, incluso si ha actualizado el clúster a la versión 1.14 o posterior, es posible que estos permisos sigan vigentes. Se recomienda que desasocie estos permisos del grupo `system:unauthenticated`.

Para obtener más información sobre la eliminación de estos permisos, consulte [Clústeres de Amazon EKS seguros con prácticas recomendadas](#) en la Guía del usuario de Amazon EKS.

Posibles problemas de configuración

Si un resultado indica un problema de configuración, consulte la sección de corrección de ese resultado para obtener directrices sobre cómo resolver ese problema concreto. Para obtener más información, consulte los siguientes tipos de resultados que indican problemas de configuración:

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- Cualquier resultado que termine en `SuccessfulAnonymousAccess`

Corregir usuarios de Kubernetes potencialmente comprometidos

Un resultado de GuardDuty puede indicar que un usuario de Kubernetes está en peligro cuando un usuario identificado en el resultado ha llevado a cabo una acción de la API inesperada. Puede identificar el usuario en la sección Detalles del usuario de Kubernetes de los detalles de un resultado en la consola o en `resource.kubernetesDetails.kubernetesUserDetails` del JSON de resultados. Estos detalles del usuario incluyen `user name`, `uid` y los grupos de Kubernetes a los que pertenece el usuario.

Si el usuario accedía a la carga de trabajo mediante una entidad de IAM, puede utilizar la sección `Access Key details` para identificar los detalles de un usuario o rol de IAM. Consulte los siguientes tipos de usuarios y sus directrices de corrección.

 Note

Puede utilizar Amazon Detective para investigar más el rol de IAM o el usuario identificado en el resultado. Mientras consulta los detalles del resultado en la consola de GuardDuty, seleccione Investigar en Detective. A continuación, seleccione el usuario de AWS o el rol de los elementos de la lista para investigarlo en Detective.

Administrador de Kubernetes integrado: usuario predeterminado asignado por Amazon EKS a la identidad de IAM que creó el clúster. Este tipo de usuario se identifica mediante el nombre de usuario `kubernetes-admin`.

Revocación del acceso de un administrador de Kubernetes integrado:

- Identifique el valor de `userType` en la sección `Access Key details`.
 - Si `userType` es Rol y el rol pertenece a un rol de instancia de EC2:
 - Identifique esa instancia y, a continuación, siga las instrucciones que se indican en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).
 - Si `userType` es Usuario o es un rol que ha asumido un usuario:
 1. [Rote la clave de acceso](#) de ese usuario.
 2. Rote los secretos a los que haya accedido el usuario.
 3. Consulte [My Cuenta de AWS account may be compromised](#) para obtener más información.

Usuario autenticado de OIDC: usuario al que se ha concedido acceso a través de un proveedor de OIDC. Normalmente, un usuario de OIDC tiene una dirección de correo electrónico como nombre de usuario. Puede comprobar si el clúster usa OIDC con el siguiente comando: `aws eks list-identity-provider-configs --cluster-name your-cluster-name`

Revocación del acceso de un usuario autenticado de OIDC:

1. Rote las credenciales de ese usuario en el proveedor de OIDC.
2. Rote los secretos a los que haya accedido el usuario.

Usuario definido por ConfigMap AWS-Auth: usuario de IAM al que se concedió acceso a través de un ConfigMap AWS-auth. Para obtener más información, consulte [Administración de usuarios o roles de IAM para su clúster](#) en la Guía del usuario de Amazon EKS. Puede revisar sus permisos con el siguiente comando: `kubectl edit configmaps aws-auth --namespace kube-system`

Para revocar el acceso de un usuario de ConfigMap de AWS:

1. Utilice el comando siguiente para abrir el ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifique la entrada de rol o usuario en la sección `mapRoles` o `mapUsers` con el mismo nombre de usuario que el indicado en la sección Detalles de usuario de Kubernetes de su resultado de GuardDuty. Consulte el siguiente ejemplo, en el que se ha identificado al usuario administrador en un resultado.

```
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. Elimine dicho usuario del ConfigMap. Consulte el siguiente ejemplo, en el que se ha eliminado el usuario administrador.

```
apiVersion: v1
data:
  mapRoles: |
```

```

- rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE306UCF
  username: system:node:{{EC2PrivateDNSName}}
  groups:
    - system:bootstrappers
    - system:nodes
mapUsers: |
- userarn: arn:aws:iam::111122223333:user/ops-user
  username: ops-user
  groups:
    - system:masters

```

4. Si userType es Usuario o es un rol que ha asumido un usuario:
 - a. [Rote la clave de acceso](#) de ese usuario.
 - b. Rote los secretos a los que haya accedido el usuario.
 - c. Consulte [My AWS account may be compromised](#) para obtener más información.

Si el resultado no tiene una sección `resource.accessKeyDetails`, el usuario es una cuenta de servicio de Kubernetes.

Cuenta de servicio: la cuenta de servicio proporciona una identidad para los pods y se puede identificar mediante un nombre de usuario con el siguiente formato:
`system:serviceaccount:namespace:service_account_name`.

Para revocar el acceso a una cuenta de servicio:

1. Cambie las credenciales de la cuenta de servicio.
2. Consulte las directrices sobre el peligro de los pods en la siguiente sección.

Corregir pods de Kubernetes potencialmente comprometidos

Cuando GuardDuty especifica detalles de un pod o recurso de carga de trabajo dentro de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails`, significa que ese pod o recurso de carga de trabajo ha sido potencialmente comprometido. Un resultado de GuardDuty puede indicar que un solo pod se ha puesto en peligro o que varios pods se han puesto en peligro a través de un recurso de nivel superior. Consulte los siguientes escenarios de peligro para obtener directrices sobre cómo identificar el pod o los pods que se han puesto en peligro.

Pods individuales en peligro

Si el campo `type` de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails` es `Pods`, el resultado identifica un solo pod. El campo `name` es el nombre de los pods y el campo `namespace` es su espacio de nombres.

Para obtener información sobre la identificación del nodo de trabajo que ejecuta los pods, consulte [Identifique el pod y el nodo de trabajo infractores](#) en la Guía de prácticas recomendadas de Amazon EKS.

Pods en peligro a través de un recurso de carga de trabajo

Si el campo `type` de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails` identifica un recurso de carga de trabajo, como `Deployment`, es probable que todos los pods de ese recurso de carga de trabajo estén en peligro.

Para obtener información sobre cómo identificar todos los pods del recurso de carga de trabajo y los nodos en los que se ejecutan, consulte [Identifique los pods y los nodos de trabajo infractores utilizando el nombre de la carga de trabajo](#) en la Guía de prácticas recomendadas de Amazon EKS.

Pods en peligro a través de una cuenta de servicio

Si un resultado de GuardDuty identifica una cuenta de servicio en la sección `resource.kubernetesDetails.kubernetesUserDetails`, es probable que los pods que utilizan la cuenta de servicio identificada estén en peligro. El nombre de usuario indicado en un resultado es una cuenta de servicio si tiene el siguiente formato: `system:serviceaccount:namespace:service_account_name`.

Para obtener información sobre la identificación de todos los pods que utilizan la cuenta de servicio y los nodos en los que se ejecutan, consulte [Identifique los pods y los nodos de trabajo infractores mediante el nombre de la cuenta de servicio](#) en la Guía de prácticas recomendadas de Amazon EKS.

Una vez que haya identificado todos los pods comprometidos y los nodos en los que se ejecutan, consulte [Aísle el pod creando una política de red que deniegue todo el tráfico de entrada y salida al pod](#) en la Guía de prácticas recomendadas de Amazon EKS.

Para corregir un pod potencialmente comprometido:

1. Identifique la vulnerabilidad que puso en peligro a los pods.
2. Implemente la corrección para esa vulnerabilidad e inicie nuevos pods de reemplazo.
3. Elimine los pods vulnerables.

Para obtener más información, consulte [Vuelva a implementar el pod o el recurso de carga de trabajo comprometido](#) en la Guía de prácticas recomendadas de Amazon EKS.

Si al nodo de trabajo se le ha asignado un rol de IAM que permite a los pods acceder a otros recursos de AWS, elimine dichos roles de la instancia para evitar que el ataque cause más daños. Del mismo modo, si al pod se le ha asignado un rol de IAM, evalúe si puede eliminar de forma segura las políticas de IAM del rol sin que ello afecte a otras cargas de trabajo.

Corregir imágenes de contenedores potencialmente comprometidas

Cuando un resultado de GuardDuty indica que un pod está comprometido, es posible que la imagen utilizada para lanzar el pod sea potencialmente maliciosa o esté comprometida. Los resultados de GuardDuty identifican la imagen de contenedor en el campo `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image`. Para determinar si la imagen es malintencionada, analícela en busca de malware.

Para corregir una imagen de contenedor potencialmente comprometida:

1. Deje de usar la imagen inmediatamente y elimínela del repositorio de imágenes.
2. Identifique todos los pods que utilizan la imagen potencialmente comprometida.

Para obtener más información, consulte [Identificar los pods con imágenes y nodos de trabajo vulnerables o comprometidos](#) en la Guía de prácticas recomendadas de Amazon EKS.

3. Aísle los pods potencialmente comprometidos, rote las credenciales y recopile datos para su análisis. Para obtener más información, consulte [Aislar el pod mediante la creación de una política de red que deniegue todo el tráfico de entrada y salida al pod en la Guía](#) de prácticas recomendadas de Amazon EKS.
4. Elimine todos los pods que utilicen la imagen potencialmente comprometida.

Corregir nodos de Kubernetes potencialmente comprometidos

Un resultado de GuardDuty puede indicar un nodo en peligro si el usuario identificado en el resultado representa la identidad de un nodo o si el resultado indica el uso de un contenedor privilegiado.

La identidad del usuario es un nodo de trabajo si el campo `username` tiene el siguiente formato: `system:node:node name`. Por ejemplo, `system:node:ip-192-168-3-201.ec2.internal`. Esto indica que el adversario ha obtenido acceso al nodo y está utilizando las credenciales del nodo para comunicarse con el punto de conexión de la API de Kubernetes.

Un resultado indica el uso de un contenedor privilegiado si uno o varios de los contenedores enumerados en el resultado tienen el campo de resultado `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext` establecido en `True`.

Para corregir un nodo potencialmente comprometido:

1. Aísle el pod, rote sus credenciales y recopile datos para el análisis forense.

Para obtener más información, consulte [Aislar el pod mediante la creación de una política de red que deniegue todo el tráfico de entrada y salida al pod en la Guía](#) de prácticas recomendadas de Amazon EKS.

2. Identifique las cuentas de servicio utilizadas por todos los pods que se ejecutan en el nodo potencialmente comprometido. Revise sus permisos y rote las cuentas de servicio si es necesario.
3. Termine el nodo potencialmente comprometido.

Corregir los resultados de la Supervisión en tiempo de ejecución

Al habilitar la Supervisión en tiempo de ejecución para la cuenta, Amazon GuardDuty puede generar [Tipos de resultados de la supervisión en tiempo de ejecución de GuardDuty](#) que indiquen posibles problemas de seguridad en el entorno de AWS. Los posibles problemas de seguridad indican que en el entorno de AWS hay una instancia de Amazon EC2, una carga de trabajo de contenedor, un clúster de Amazon EKS o un conjunto de credenciales comprometidos. El agente de seguridad supervisa los eventos en tiempo de ejecución de varios tipos de recursos. Para identificar el recurso potencialmente en peligro, consulte Tipo de recurso en los detalles del resultado generado en la consola de GuardDuty. En la siguiente sección se describen los pasos de corrección recomendados para cada tipo de recurso.

Instance

Si el tipo de recurso en los detalles del resultado es Instancia, indica que una instancia de EC2 o un nodo de EKS están potencialmente en peligro.

- Para corregir un nodo de EKS en peligro, consulte [Corregir nodos de Kubernetes potencialmente comprometidos](#).
- Para corregir una instancia de EC2 en peligro, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

EKSCluster

Si el tipo de recurso en los detalles del resultado es EKSCluster, indica que un pod o un contenedor de un clúster de EKS están potencialmente en peligro.

- Para corregir un pod en peligro, consulte [Corregir pods de Kubernetes potencialmente comprometidos](#).
- Para corregir una imagen de contenedor en peligro, consulte [Corregir imágenes de contenedores potencialmente comprometidas](#).

ECSCluster

Si el tipo de recurso en los detalles del resultado es ECSCluster, significa que una tarea de ECS o un contenedor dentro de una tarea de ECS está potencialmente comprometido.

1. Identifique el clúster de ECS afectado

El resultado de la Supervisión en tiempo de ejecución de GuardDuty proporciona los detalles del clúster de ECS en el panel de detalles del resultado o en la sección `resource.ecsClusterDetails` del JSON del resultado.

2. Identifique la tarea de ECS afectada

El resultado de la Supervisión en tiempo de ejecución de GuardDuty proporciona los detalles de la tarea de ECS en el panel de detalles del resultado o en la sección `resource.ecsClusterDetails.taskDetails` del JSON del resultado.

3. Aísle la tarea afectada

Para aislar la tarea impactada, deniegue todo el tráfico de entrada y salida a la tarea. Una regla que prohíba todo el tráfico puede ayudar a detener un ataque que ya está en marcha, ya que interrumpe todas las conexiones con la tarea.

4. Corrija la tarea comprometida

- a. Identifique la vulnerabilidad que comprometió la tarea.
- b. Implemente la corrección de esa vulnerabilidad e inicie una nueva tarea de sustitución.
- c. Detenga la tarea vulnerable.

Container

Si el tipo de recurso en los detalles del resultado es Contenedor, indica que un contenedor independiente está potencialmente en peligro.

- Para corregirlo, consulte [Corregir un contenedor independiente potencialmente comprometido](#).
- Si el resultado se genera en varios contenedores con la misma imagen de contenedor, consulte [Corregir imágenes de contenedores potencialmente comprometidas](#).
- Si el contenedor ha accedido al host de EC2 subyacente, es posible que las credenciales de la instancia asociadas se hayan puesto en peligro. Para obtener más información, consulte [Corregir credenciales de AWS potencialmente comprometidas](#).
- Si un agente potencialmente malintencionado ha accedido al nodo de EKS subyacente o a una instancia de EC2, consulte la corrección recomendada en las pestañas EKSCluster e Instancia.

Corrección de imágenes de contenedor en peligro

Cuando un resultado de GuardDuty indica que una tarea está comprometida, es posible que la imagen utilizada para lanzar la tarea sea maliciosa o esté comprometida.

Los resultados de GuardDuty identifican la imagen de contenedor en el campo `resource.ecsClusterDetails.taskDetails.containers.image`. Para determinar si la imagen es maliciosa o no, puede analizarla en busca de malware.

Para corregir una imagen de contenedor comprometida

1. Deje de usar la imagen inmediatamente y elimínela del repositorio de imágenes.
2. Identifique todas las tareas que utilizan esta imagen.

3. Detenga todas las tareas que utilizan la imagen comprometida. Actualice las definiciones de las tareas de modo que dejen de utilizar la imagen comprometida.

Corregir una base de datos potencialmente comprometida

GuardDuty genera [Tipos de resultados de la protección de RDS](#) que indican un comportamiento de inicio de sesión potencialmente sospechoso y anómalo en las [Bases de datos compatibles](#) después de habilitar la [Protección de RDS](#). Con la actividad de inicio de sesión de RDS, GuardDuty identifica patrones atípicos en los intentos de inicio de sesión para analizar y describir las amenazas.

Note

Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la [Tipos de resultados activos de GuardDuty](#).

Siga estos pasos recomendados para corregir una base de datos de Amazon Aurora potencialmente en peligro en su entorno de AWS.

Temas

- [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#)
- [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#)
- [Corrección de credenciales potencialmente en peligro](#)
- [Restricción del acceso a la red](#)

Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos

Los siguientes pasos recomendados pueden ayudarlo a corregir una base de datos de Aurora potencialmente en peligro que presenta un comportamiento atípico en relación con los eventos de inicio de sesión correctos.

1. Identifique la base de datos y el usuario afectados.

El resultado de GuardDuty generado proporciona el nombre de la base de datos afectada y los detalles del usuario correspondientes. Para obtener más información, consulte [Detalles de los resultados](#).

2. Confirme si este comportamiento es esperado o inesperado.

En la siguiente lista se especifican los posibles escenarios que pueden haber provocado que GuardDuty genere un resultado:

- Un usuario que inicia sesión en su base de datos después de un largo periodo de tiempo.
- Un usuario que inicia sesión en su base de datos de forma ocasional (por ejemplo, un analista financiero que inicia sesión cada trimestre).
- Un agente potencialmente sospechoso que participa en un intento de inicio de sesión correcto podría poner en peligro la base de datos.

3. Comience este paso si el comportamiento es inesperado.

1. Restrinja el acceso a la base de datos

Restrinja el acceso a la base de datos para las cuentas sospechosas y el origen de esta actividad de inicio de sesión. Para obtener más información, consulte [Corrección de credenciales potencialmente en peligro](#) y [Restricción del acceso a la red](#).

2. Evalúe el impacto y determine a qué información se accedió.

- Si están disponibles, revise los registros de auditoría para identificar los datos a los que se puede haber accedido. Para obtener más información, consulte [Supervisión de eventos, registros y flujos en un clúster de bases de datos de Amazon Aurora](#) en la Guía del usuario de Amazon Aurora.
- Determine si se accedió a información confidencial o protegida o si se modificó.

Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos

Los siguientes pasos recomendados pueden ayudarlo a corregir una base de datos de Aurora potencialmente en peligro que presenta un comportamiento atípico en relación con los eventos de inicio de sesión fallidos.

1. Identifique la base de datos y el usuario afectados.

El resultado de GuardDuty generado proporciona el nombre de la base de datos afectada y los detalles del usuario correspondientes. Para obtener más información, consulte [Detalles de los resultados](#).

2. Identifique el origen de los intentos de inicio de sesión fallidos.

El resultado de GuardDuty generado proporciona la dirección IP y la organización de ASN (si se trataba de una conexión pública) en la sección Actor del panel de resultados.

Un sistema autónomo (AS) es un grupo de uno o varios prefijos de IP (listas de direcciones IP accesibles en una red) administrado por uno o más operadores de red que mantienen una política de enrutamiento única y claramente definida. Los operadores de red necesitan números de sistemas autónomos (ASN) para controlar el enrutamiento en sus redes e intercambiar información de enrutamiento con otros proveedores de servicios de internet (ISP).

3. Confirme que este comportamiento es inesperado.

Examine si esta actividad representa un intento de obtener acceso adicional no autorizado a la base de datos de la siguiente manera:

- Si el origen es interno, compruebe si una aplicación está mal configurada y si está intentando conectarse repetidamente.
- Si se trata de un agente externo, compruebe si la base de datos correspondiente es pública o está mal configurada y, por lo tanto, permite que posibles actores malintencionados utilicen nombres de usuario comunes por fuerza bruta.

4. Comience este paso si el comportamiento es inesperado.

1. Restrinja el acceso a la base de datos.

Restrinja el acceso a la base de datos para las cuentas sospechosas y el origen de esta actividad de inicio de sesión. Para obtener más información, consulte [Corrección de credenciales potencialmente en peligro](#) y [Restricción del acceso a la red](#).

2. Analice la causa raíz y determine los pasos que podrían haber llevado a esta actividad.

Configure una alerta para recibir una notificación cuando una actividad modifique una política de red y cree un estado no seguro. Para obtener más información, consulte [Firewall policies in AWS Network Firewall](#) en la Guía para desarrolladores de AWS Network Firewall.

Corrección de credenciales potencialmente en peligro

Un resultado de GuardDuty puede indicar que las credenciales de usuario de una base de datos afectada se han puesto en peligro cuando el usuario identificado en el resultado ha llevado a cabo una operación inesperada en la base de datos. Puede identificar el usuario en la sección Detalles del usuario de base de datos de RDS del panel de resultados de la consola o en `resource.rdsDbUserDetails` del JSON de resultados. Estos detalles del usuario incluyen el nombre de usuario, la aplicación utilizada, la base de datos a la que se ha accedido, la versión de SSL y el método de autenticación.

- Para revocar el acceso o rotar las contraseñas de usuarios específicos que participan en el resultado, consulte [Seguridad con Amazon Aurora MySQL](#) o [Seguridad con Amazon Aurora PostgreSQL](#) en la Guía del usuario de Amazon Aurora.
- Utilice AWS Secrets Manager para almacenar de forma segura y rotar automáticamente los secretos de bases de datos de Amazon Relational Database Service (RDS). Para obtener más información, consulte [Tutoriales de AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager.
- Utilice la autenticación de bases de datos de IAM para administrar el acceso de los usuarios a las bases de datos sin necesidad de contraseñas. Para obtener más información, consulte [Autenticación de bases de datos de IAM](#) en la Guía del usuario de Amazon Aurora.

Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon Relational Database Service](#) en la Guía del usuario de Amazon RDS.

Restricción del acceso a la red

Un resultado de GuardDuty puede indicar que se puede acceder a una base de datos más allá de sus aplicaciones o de la nube privada virtual (VPC). Si la dirección IP remota del resultado es un origen de conexión inesperado, audite los grupos de seguridad. Encontrará una lista de los grupos de seguridad adjuntos a la base de datos en Grupos de seguridad, en la consola <https://console.aws.amazon.com/rds/> o en `resource.rdsDbInstanceDetails.dbSecurityGroups` del JSON de resultados. Para obtener más información sobre la configuración de los grupos de seguridad, consulte [Control de acceso con grupos de seguridad](#) en la Guía del usuario de Amazon RDS.

Si utiliza un firewall, restrinja el acceso a la red a la base de datos; para ello, reconfigure las listas de control de acceso a la red (NACL). Para obtener más información, consulte [Firewall in AWS Network Firewall](#) en la Guía para desarrolladores de AWS Network Firewall.

Corregir una función de Lambda potencialmente comprometida

Cuando GuardDuty genera [Tipos de resultados de la protección de Lambda](#), es posible que la función de Lambda se haya visto comprometida. Si la actividad que causó que GuardDuty generara este resultado era esperada, puede considerar usar [Reglas de supresión](#). Recomendamos completar los siguientes pasos para corregir una función de Lambda comprometida:

Corrección de los resultados de la protección de Lambda

1. Identifique la versión de la función Lambda potencialmente comprometida.

Un resultado de GuardDuty para la protección de Lambda proporciona el nombre, el Nombre de recurso de Amazon (ARN), la versión de la función y el ID de revisión asociados a la función de Lambda que aparecen en los detalles del resultado.

2. Identifique el origen de la actividad potencialmente sospechosa.
 - a. Revise el código asociado a la versión de la función de Lambda implicada en el resultado.
 - b. Revise las bibliotecas y capas importadas de la versión de la función de Lambda implicada en el resultado.
 - c. Si ha habilitado el [análisis de las funciones de AWS Lambda con Amazon Inspector](#), revise los [resultados de Amazon Inspector](#) asociados a la función de Lambda implicada en el resultado.
 - d. Revise los registros de AWS CloudTrail para identificar la entidad principal que provocó la actualización de la función y asegúrese de que la actividad estaba autorizada o prevista.
3. Corrija la función de Lambda potencialmente comprometida.
 - a. Deshabilite los desencadenadores de ejecución de la función de Lambda implicada en el resultado. Para obtener más información, consulte [DeleteFunctionEventInvokeConfig](#).
 - b. Revise el código de Lambda y actualice las importaciones de bibliotecas y las [capas de la función de Lambda](#) para eliminar las bibliotecas y las capas potencialmente sospechosas.
 - c. Mitigue los resultados de Amazon Inspector relacionados con la función de Lambda implicada en el resultado.

Estimar el costo de uso de GuardDuty

Durante la prueba gratuita de 30 días, puede utilizar la consola de GuardDuty o las operaciones de la API para estimar el promedio diario de los costos de uso de GuardDuty. La estimación de costos proyecta cuáles serán los costos estimados después del periodo de prueba. Sin embargo, para revisar una estimación precisa de los costos durante la prueba gratuita, GuardDuty recomienda utilizar AWS Billing en <https://console.aws.amazon.com/costmanagement/>.

Cuando se opera en un entorno de varias cuentas, la cuenta de administrador de GuardDuty puede supervisar las métricas de costos correspondientes a todas las cuentas de miembro.

Nota sobre el costo de uso de la protección contra malware para S3

El costo de uso de la protección contra malware para S3 no está incluido bajo Uso en la consola de GuardDuty. Para obtener más información, consulte [Revisar el costo de uso de la protección contra malware para S3](#).

Puede ver la estimación de costos en función de las siguientes métricas:

- ID de cuenta: indica el costo estimado de su cuenta o de sus cuentas de miembros si opera como una cuenta de administrador de GuardDuty.
- Orígenes de datos: enumera el costo estimado de todos los eventos de administración de [Orígenes de datos fundamentales](#) - AWS CloudTrail, registros de flujo de VPC y registros de consultas de DNS de Route53 Resolver.
- Características: enumera el costo estimado de las [características de GuardDuty](#): eventos de datos de CloudTrail para S3, supervisión del registro de auditoría de EKS, datos de volúmenes de EBS, actividad de inicio de sesión en RDS, Supervisión en tiempo de ejecución de EKS, Supervisión en tiempo de ejecución de Fargate, Supervisión en tiempo de ejecución de EC2 o Supervisión de actividad de red de Lambda.
- Buckets de S3: indica el costo estimado de los eventos de datos de S3 en un bucket específico o en los buckets más caros de las cuentas de su entorno. Esta estadística solo está disponible cuando se habilita [Protección de S3](#) para una Cuenta de AWS.

Descripción de cómo calcula GuardDuty los costos de uso

Las estimaciones que se muestran en la consola de GuardDuty pueden diferir ligeramente de las de la consola de Administración de facturación y costos de AWS. En la lista siguiente se explica cómo estima GuardDuty los costos de uso:

- La estimación de uso de GuardDuty es solo para la región actual.
- El costo de uso de GuardDuty se basa en los últimos 30 días de uso.
- La estimación del costo de uso de la versión de prueba incluye la estimación de las características y los orígenes de datos básicos que se encuentran actualmente en el periodo de prueba. Cada característica y origen de datos de GuardDuty tiene su propio periodo de prueba, pero puede coincidir con el periodo de prueba de GuardDuty u otra característica que se haya habilitado al mismo tiempo.
- La estimación de uso de GuardDuty incluye descuentos en los precios por volumen de GuardDuty por región, tal como se detalla en la página [Precios de Amazon GuardDuty](#), pero solo en el caso de cuentas individuales que cumplan con los niveles de precios por volumen. Los descuentos en los precios por volumen no se incluyen en las estimaciones del uso total combinado entre las cuentas de una organización. Para obtener información sobre los precios con descuentos por volumen de uso combinado, consulte [Facturación de AWS: descuentos por volumen](#).
- Es posible que la suma del costo de uso de cada Cuenta de AWS de la organización no siempre coincida con el costo estimado de los últimos 30 días para el origen de datos seleccionado. Es posible que el nivel de precios cambie a medida que GuardDuty procese más eventos o datos. Para obtener más información, consulte [Niveles de precios](#) en la Guía del usuario de AWS Billing.

Este escenario explica que, para dejar de incurrir en costos de uso por la Supervisión en tiempo de ejecución, debe desactivar las características de Supervisión en tiempo de ejecución y Supervisión en tiempo de ejecución de EKS.

GuardDuty ha consolidado la experiencia de la consola para la Supervisión en tiempo de ejecución de EKS en la Supervisión en tiempo de ejecución. GuardDuty recomienda [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#) y [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#).

Como parte de la migración a la Supervisión en tiempo de ejecución, asegúrese de [Desactivar la Supervisión en tiempo de ejecución de EKS](#). Esto es importante porque si más adelante decide

desactivar la Supervisión en tiempo de ejecución y no desactiva la Supervisión en tiempo de ejecución de EKS, no dejará de incurrir en costos por el uso de la Supervisión en tiempo de ejecución de EKS.

Supervisión en tiempo de ejecución: cómo los registros de flujo de VPC de las instancias de EC2 afectan al costo de uso

Al administrar el agente de seguridad (ya sea manualmente o a través de GuardDuty) en la Supervisión en tiempo de ejecución de EKS o en la Supervisión en tiempo de ejecución para instancias de EC2, y GuardDuty se encuentre actualmente implementado en una instancia de Amazon EC2 y recibe el [Tipos de eventos de tiempo de ejecución recopilados](#) de esta instancia, GuardDuty no cobrará a la Cuenta de AWS por el análisis de los registros de flujo de la VPC procedentes de esta instancia de Amazon EC2. Esto ayuda a GuardDuty a evitar el doble costo de uso en la cuenta.

Cómo estima GuardDuty el costo del uso de los eventos de CloudTrail

Al habilitar GuardDuty, automáticamente comienza a consumir registros de eventos de AWS CloudTrail registrados para su cuenta en la Región de AWS seleccionada. GuardDuty replica los registros de [eventos del servicio global](#) y, a continuación, los procesa de forma independiente en cada región en la que haya habilitado GuardDuty. Esto ayuda a GuardDuty a mantener los perfiles de usuarios y roles en cada región para identificar anomalías.

La configuración de CloudTrail no afecta al costo del uso de GuardDuty ni a la forma en que GuardDuty procesa los registros de eventos. El costo del uso de GuardDuty se ve afectado por el uso de las API de AWS que registran en CloudTrail. Para obtener más información, consulte [Eventos de administración de AWS CloudTrail](#).

Revisar el costo estimado de uso de GuardDuty

El uso de GuardDuty proporciona estimaciones de costos basadas en el uso de los últimos 30 días por Región de AWS. El uso estimado es diferente del uso facturado. Para obtener información sobre cómo GuardDuty calcula el costo de uso, consulte [Descripción de cómo calcula GuardDuty los costos de uso](#). Si es una cuenta de administrador de GuardDuty, puede ver las estimaciones de costos para cada cuenta de miembro, desglosadas por orígenes de datos y cuentas.

Elija el método de acceso que prefiera para revisar el costo de uso de la cuenta de GuardDuty.

Para revisar el costo estimado de uso de GuardDuty

Console

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de usar la cuenta de administrador de GuardDuty.

2. En el panel de navegación, seleccione Uso.
3. En la página Uso, una cuenta de administrador de GuardDuty con cuentas de miembro puede ver el Costo estimado de la organización correspondiente a los últimos 30 días. Se trata de un costo de uso total estimado para la organización.
4. Las cuentas de administrador de GuardDuty pueden ver el desglose de costos de uso por orígenes de datos, o por cuentas. Las cuentas individuales o independientes pueden ver el desglose por orígenes de datos.

Si tiene cuentas de miembro: seleccione la pestaña Por cuentas para ver las estadísticas de cada cuenta de miembro.

En la pestaña Por orígenes de datos, al seleccionar un origen de datos con un costo de uso asociado, es posible que la suma correspondiente en el desglose de costos a nivel de cuentas no sea siempre la misma.

API/CLI

Ejecute la operación de la API [GetUsageStatistics](#) con las credenciales de la cuenta de administrador de GuardDuty. Proporcione la siguiente información para ejecutar el comando:

- (Obligatorio) Proporcione el ID del detector de GuardDuty regional de la cuenta para la que desea recuperar las estadísticas.
- (Obligatorio) Proporcione uno de los tipos de estadísticas que desee recuperar:
SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE
| TOP_ACCOUNTS_BY_FEATURE.

Actualmente, TOP_ACCOUNTS_BY_FEATURE no admite la recuperación de estadísticas de uso de RDS_LOGIN_EVENTS.

- (Obligatorio) proporcione uno o más orígenes de datos o características para consultar las estadísticas de uso.
- (Opcional) Proporcione una lista de los ID de cuentas de los que desea recuperar las estadísticas de uso.

También puede utilizar la AWS Command Line Interface. El siguiente comando es un ejemplo de cómo recuperar las estadísticas de uso correspondientes a todos los orígenes de datos y características, calculadas por cuentas. Asegúrese de sustituir `detector-id` por su propio ID de detector válido. En el caso de las cuentas independientes, este comando devuelve el costo del uso de los últimos 30 días únicamente para su cuenta. Si es una cuenta de administrador de GuardDuty con cuentas de miembro, verá los costos enumerados por cuenta correspondientes a todos los miembros.

Para encontrar el `detectorId` correspondiente a la cuenta y la región actual, consulte la página de Configuración en la consola <https://console.aws.amazon.com/guardduty/> o ejecute la API [ListDetectors](#).

Sustituya `SUM_BY_ACCOUNT` por el tipo con el que desea calcular las estadísticas de uso.

Para supervisar únicamente el costo correspondiente a los orígenes de datos

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
"EC2_MALWARE_SCAN"]}'
```

Para supervisar el costo correspondiente a las características

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
"EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
"EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Nombres de características para planes de protección en la API de GuardDuty

Al habilitar Amazon GuardDuty por primera vez, comienza a procesar [Orígenes de datos fundamentales](#) dentro del entorno de AWS. GuardDuty utiliza estos orígenes de datos para procesar una secuencia independiente de eventos, como registros de flujo de VPC, registros de DNS y eventos de administración de AWS CloudTrail. A continuación, analiza estos eventos para identificar posibles amenazas de seguridad y genera resultados en su cuenta.

Cuando uno o más planes de protección están habilitados, GuardDuty utiliza datos adicionales de otros servicios de AWS en el entorno de AWS para supervisar y analizar posibles amenazas a la seguridad. Estos orígenes de datos adicionales se denominan características.

Cambio de orígenes de datos a características

Cuando se agregan protecciones adicionales de GuardDuty, como la protección de S3, la Supervisión en tiempo de ejecución, la protección de Lambda y otras, se puede configurar la característica de GuardDuty correspondiente al plan de protección. Históricamente, las protecciones de GuardDuty se denominaban `dataSources` en las API. Sin embargo, desde marzo de 2023, los nuevos planes de protección de GuardDuty ahora se configuran como `features` y no como `dataSources`. GuardDuty aún permite configurar planes de protección lanzados antes de marzo de 2023 como `dataSources` a través de la API. Sin embargo, los nuevos planes de protección solo están disponibles como `features`. Para obtener información sobre los planes de protección que se ven afectados, consulte [Cambios en la API de GuardDuty](#).

Si administra la configuración y los planes de protección de GuardDuty a través de la consola, este cambio no le afecta directamente y no necesita tomar ninguna medida. Este cambio afecta el comportamiento de las API que se invocan para habilitar GuardDuty o planes de protección dentro de GuardDuty. Si utiliza API o AWS CLI para habilitar o editar la configuración de un plan de protección, debe utilizar el nombre de la característica asociada. Para obtener más información, consulte [Asignación de `dataSources` a `features`](#).

Cambios en la API de GuardDuty en marzo de 2023

Las API de GuardDuty configuran características de protección que no pertenecen a la lista de [Orígenes de datos fundamentales de GuardDuty](#). Un objeto de característica contiene detalles de

la característica, como el nombre y el estado de la característica, y puede contener configuración adicional para algunos de los planes de protección. Esta migración afecta a las siguientes API de la Referencia de la API de Amazon GuardDuty:

- [CreateDetector](#)
- [GetDetector](#)
- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

Características en comparación con los orígenes de datos

Históricamente, todas las características de GuardDuty se pasaban a través de un objeto `dataSources` de la API. A partir de marzo de 2023, GuardDuty prefiere el objeto `features` en lugar del objeto `dataSources` en la API. Todos los orígenes de datos anteriores tienen las características correspondientes, pero es posible que las características más recientes no tengan los orígenes de datos correspondientes.

En la siguiente lista se muestra la comparación entre los objetos `dataSources` y `features` cuando se pasan a través de una API:

- El objeto `dataSources` contiene objetos para cada tipo de protección y su estado. El objeto `features` es una lista de características disponibles que corresponden a cada tipo de protección de GuardDuty.

A partir de marzo de 2023, la activación de características será la única forma de configurar las nuevas características de GuardDuty en su entorno de AWS.

- El esquema `dataSources` de la solicitud o respuesta de la API es el mismo en todas las Región de AWS en las que GuardDuty está disponible. Sin embargo, es posible que no todas las características estén disponibles en todas las regiones. Por lo tanto, los nombres de las características disponibles pueden variar según la región.

Comprender cómo funcionan las API con características

Las API de GuardDuty seguirán devolviendo un objeto `dataSources` según proceda y también devolverán un objeto `features` con la misma información en un formato diferente. Las características de GuardDuty lanzadas antes de marzo de 2023 estarán disponibles a través de los objetos `dataSources` y `features`. Las características de GuardDuty lanzadas desde de marzo de 2023 solo estarán disponibles a través del objeto `features`. No puede crear ni actualizar un detector, ni describir su organización de AWS Organizations con la notación de los objetos `dataSources` y `features` en la misma solicitud de la API. Para habilitar los tipos de protecciones de GuardDuty, tendrá que migrar los orígenes de datos existentes al objeto `features` con las mismas API que ahora también incluyen el objeto `features`.

Note

GuardDuty no agregará un nuevo origen de datos después de esta modificación.

GuardDuty ha dejado obsoleto el uso de orígenes de datos asociados a los planes de protección. Sin embargo, sigue admitiendo los [Orígenes de datos fundamentales de GuardDuty](#). Las prácticas recomendadas de GuardDuty sugieren el uso de características para habilitar o editar la configuración de cualquier plan de protección en la cuenta.

Incorporar cambios de características en las API

- Si administra las configuraciones de GuardDuty a través de API, SDK o plantillas de CloudFormation y desea habilitar posibles características nuevas de GuardDuty, tendrá que modificar el código y la plantilla, respectivamente. Para obtener más información, consulte las API actualizadas en la [Referencia de la API de Amazon GuardDuty](#).
- En el caso de las características de GuardDuty configuradas antes de esta actualización, puede seguir utilizando las API, los SDK o la plantilla de CloudFormation. Sin embargo, le recomendamos que cambie para usar el objeto `feature`.

Todos los orígenes de datos tienen un objeto de característica equivalente. Para obtener más información, consulte [Asignación de `dataSources` a `features`](#).

- Actualmente, `additionalConfiguration` en el objeto `features` solo está disponible para ciertos tipos de protecciones.

- Para estos tipos de protecciones, si el valor de `status` de `AdditionalConfiguration` de la característica está establecido en `ENABLED`, pero el valor de `status` de la configuración de la característica no está establecido en `ENABLED`, GuardDuty no llevará a cabo ninguna acción en este caso.
- Esto afecta a las siguientes API:
 - [UpdateDetector](#)
 - [UpdateMemberDetectors](#)
 - [UpdateOrganizationConfiguration](#)

Asignación de **dataSources** a **features**

En la siguiente tabla se muestra la asignación de los tipos de protecciones, `dataSources` y `features`.

Tipo de protección de GuardDuty	Nombre del origen de datos [*]	Nombre de la característica
Logs de flujo de VPC	<code>flowLogs</code> (solo lectura; no se puede modificar)	<code>FLOW_LOGS</code> (solo lectura; no se puede modificar)
Registros de consultas de DNS de Route53 Resolver	<code>dnsLogs</code> (solo lectura; no se puede modificar)	<code>DNS_LOGS</code> (solo lectura; no se puede modificar)
Eventos de CloudTrail	<code>cloudTrail</code> (solo lectura; no se puede modificar)	<code>CLOUD_TRAIL</code> (solo lectura; no se puede modificar)
S3	<code>s3Logs</code>	<code>S3_DATA_EVENTS</code>
Protección de EKS	<code>kubernetes.auditlogs</code>	<code>EKS_AUDIT_LOGS</code>
Protección contra malware para EC2	<code>malwareProtection.scanEc2InstanceWithFindings.ebsVolumes</code>	<code>EBS_MALWARE_PROTECTION</code>

Tipo de protección de GuardDuty	Nombre del origen de datos*	Nombre de la característica
Eventos de inicio de sesión de RDS		RDS_LOGIN_EVENTS
Supervisión en tiempo de ejecución de EKS		EKS_RUNTIME_MONITORING
Supervisión en tiempo de ejecución		RUNTIME_MONITORING
Agente de seguridad GuardDuty para clústeres de Amazon EKS	GuardDuty solo admite la activación de características para estos tipos de protecciones.	EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
		RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
Agente de seguridad GuardDuty para clústeres de Amazon ECS-Fargate		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT

Tipo de protección de GuardDuty	Nombre del origen de datos [*]	Nombre de la característica
Agente de seguridad de GuardDuty para instancias de Amazon EC2		RUNTIME_MONITORING_additionalConfiguration.EC2_AGENT_MANAGEMENT
Protección de Lambda		LAMBDA_NETWORK_LOGS

^{*} GetUsageStatistics usa sus propios nombres de dataSource. Para obtener más información, consulte [Estimar el costo de uso de GuardDuty](#) o [GetUsageStatistics](#).

Seguridad en Amazon GuardDuty

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Terceros clientes prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [Programas de conformidad de AWS](#). Para obtener información sobre los programas de conformidad que se aplican a GuardDuty, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza GuardDuty. Se muestra cómo configurar GuardDuty para satisfacer sus objetivos de seguridad y conformidad. También puede obtener información sobre cómo utilizar otros servicios de AWS que lo ayuden a supervisar y proteger los recursos de GuardDuty.

Contenido

- [Protección de los datos en Amazon GuardDuty](#)
- [Registro de llamadas a la API de Amazon GuardDuty con AWS CloudTrail](#)
- [Identity and Access Management para Amazon GuardDuty](#)
- [Validación de la conformidad de Amazon GuardDuty](#)
- [Resiliencia de Amazon GuardDuty](#)
- [Seguridad de la infraestructura en Amazon GuardDuty](#)
- [Amazon GuardDuty y puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#)

Protección de los datos en Amazon GuardDuty

El [modelo de responsabilidad compartida](#) de AWS se aplica a la protección de datos en Amazon GuardDuty. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta [Working with CloudTrail trails](#) en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye las situaciones en las que debe trabajar con GuardDuty u otros Servicios de AWS mediante la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que

ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Todos los datos de los clientes de GuardDuty se cifran en reposo mediante soluciones de cifrado de AWS.

Los datos de GuardDuty, como los resultados, se cifran en reposo mediante AWS Key Management Service (AWS KMS) con claves propiedad de AWS administradas por el cliente.

Cifrado en tránsito

GuardDuty analiza los datos de registro de otros servicios. Cifra todos los datos en tránsito de estos servicios con HTTPS y KMS. Una vez que GuardDuty extrae la información que necesita de los registros, estos se descartan. Para obtener más información sobre cómo utiliza GuardDuty la información de otros servicios, consulte [GuardDuty data sources](#).

Los datos de GuardDuty se cifran en tránsito entre los servicios.

Optar por no utilizar sus datos para mejorar el servicio

Puede optar por que no se utilicen sus datos para desarrollar y mejorar GuardDuty y otros servicios de seguridad de AWS mediante la política de exclusión voluntaria de AWS Organizations. Puede optar por que se le excluya incluso si GuardDuty no recopila actualmente dichos datos. Para más información sobre cómo excluirse, consulte [Políticas de exclusión de servicios de IA](#) en la Guía del usuario de AWS Organizations.

Note

Para poder utilizar la política de exclusión voluntaria, sus cuentas de AWS las debe administrar AWS Organizations de forma centralizada. Si aún no ha creado una organización para sus cuentas de AWS, consulte [Creación y administración de una organización](#) en la Guía del usuario de AWS Organizations.

La exclusión voluntaria tiene los siguientes efectos:

- GuardDuty eliminará los datos que recopiló y almacenó con fines de mejora del servicio antes de decidir no participar (en su caso).
- Después de optar por no participar, GuardDuty ya no recopilará ni almacenará estos datos con fines de mejora del servicio.

En los siguientes temas se explica cómo cada característica dentro de GuardDuty potencialmente trata los datos para mejorar el servicio.

Contenido

- [Supervisión del tiempo de ejecución de GuardDuty](#)
- [Protección contra malware de GuardDuty](#)

Supervisión del tiempo de ejecución de GuardDuty

La Supervisión en tiempo de ejecución de GuardDuty proporciona detección de amenazas en tiempo de ejecución para clústeres de Amazon Elastic Kubernetes Service (Amazon EKS), solo para instancias de Amazon Elastic Container Service (Amazon ECS) de AWS Fargate y Amazon Elastic Compute Cloud (Amazon EC2) en el entorno de AWS. Después de habilitar la Supervisión en tiempo de ejecución e implementar el agente de seguridad de GuardDuty para el recurso, GuardDuty comienza a supervisar y analizar los eventos en tiempo de ejecución asociados al recurso. Estos tipos de eventos en tiempo de ejecución incluyen eventos de proceso, eventos de contenedor, eventos DNS y más. Para obtener más información, consulte [Tipos de eventos de tiempo de ejecución recopilados que utiliza GuardDuty](#).

GuardDuty recopila tanto los comandos (como `systemctl`, `cron` y `curl`) como sus argumentos asociados (como `start`, `stop`, `disable`) de sus cargas de trabajo. Por ejemplo, cuando alguien ejecuta `systemctl stop service-name`, GuardDuty captura tanto el comando `systemctl` como sus argumentos `stop service-name`. Esta información detallada ayuda a GuardDuty a detectar amenazas sofisticadas mediante el análisis de los patrones de comandos y la correlación de varios eventos. Por ejemplo, GuardDuty puede identificar cuándo un atacante intenta deshabilitar los servicios de seguridad o ejecuta archivos maliciosos conocidos. Aunque GuardDuty utiliza activamente estos datos para propósitos de detección de amenazas, actualmente no utiliza estos comandos y argumentos para propósitos de mejora del servicio (puede que lo haga en el futuro). Su confianza, la privacidad y la seguridad de su contenido son nuestra máxima prioridad y garantizamos que nuestro uso cumpla con nuestros compromisos con usted. Para obtener más información, consulte [Preguntas frecuentes sobre privacidad de datos](#).

Protección contra malware de GuardDuty

La protección contra malware de GuardDuty analiza y detecta el malware contenido en los volúmenes de EBS asociados a las cargas de trabajo de instancias y contenedores de Amazon EC2 potencialmente comprometidas, así como los archivos recién cargados en los buckets de Amazon S3 seleccionados. Actualmente, GuardDuty no recopila ni utiliza el malware detectado para mejorar el servicio. Sin embargo, en el futuro, cuando la protección contra malware de GuardDuty identifique un archivo de volumen de EBS o un archivo de S3 como malicioso o dañino, la protección contra malware de GuardDuty recopilará y almacenará este archivo para desarrollar y mejorar las detecciones de malware y el servicio de GuardDuty. Este archivo también se puede utilizar para desarrollar y mejorar otros servicios de seguridad de AWS. Su confianza, la privacidad y la seguridad de su contenido son nuestra máxima prioridad y garantizamos que nuestro uso cumpla con nuestros compromisos con usted. Para obtener más información, consulte [Preguntas frecuentes sobre privacidad de datos](#).

Registro de llamadas a la API de Amazon GuardDuty con AWS CloudTrail

Amazon GuardDuty se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones que ha llevado a cabo un usuario, un rol o un servicio de AWS en GuardDuty. CloudTrail captura todas las llamadas a la API de GuardDuty como eventos, incluidas las llamadas procedentes de la consola de GuardDuty y las llamadas de código a las API de este servicio. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos de GuardDuty. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se hizo a GuardDuty, la dirección IP desde la que se hizo, quién la hizo y cuándo se hizo, entre otros detalles.

Para obtener más información acerca de CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la [Guía de usuario de AWS CloudTrail](#).

Información de GuardDuty en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad de eventos compatible en GuardDuty, la actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos

eventos de la cuenta de AWS. Para obtener más información, consulte [Ver eventos con el historial de eventos de CloudTrail](#).

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de GuardDuty, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- [Introducción a la creación de registros de seguimiento](#)
- [Servicios e integraciones compatibles con CloudTrail](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones](#) y [Recibir archivos de registro de CloudTrail de varias cuentas](#)

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se hizo con las credenciales de inicio de sesión del usuario raíz o del usuario de IAM
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- si la solicitud la realizó otro servicio de AWS

Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).

Eventos del plano de control de GuardDuty en CloudTrail

De forma predeterminada, CloudTrail registra todas las operaciones de la API de GuardDuty incluidas en la [Referencia de la API de Amazon GuardDuty](#) como eventos en los archivos de CloudTrail.

Eventos de datos de GuardDuty en CloudTrail

[Supervisión del tiempo de ejecución de GuardDuty](#) utiliza un agente de seguridad de GuardDuty implementado en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS), las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y las tareas de AWS Fargate (solo Amazon Elastic Container Service [Amazon ECS]) para el complemento de recopilación (`aws-guardduty-agent`) que recopila [Tipos de eventos de tiempo de ejecución recopilados](#) para las cargas de trabajo de AWS y, a continuación, los envía a GuardDuty para la detección y el análisis de amenazas.

Registro y supervisión de eventos de datos

Si lo desea, puede configurar los registros de AWS CloudTrail para ver los eventos de datos de su agente de seguridad de GuardDuty.

Para crear y configurar CloudTrail, consulte [Data events](#) en la Guía del usuario de AWS CloudTrail y siga las instrucciones de Logging data events with advanced event selectors in the Consola de administración de AWS. Al registrar el registro de seguimiento, asegúrese de hacer los siguientes cambios:

- En Tipo de evento de datos, elija Detector de GuardDuty.
- En Plantilla de selector de registros, elija Registrar todos los eventos.
- Amplíe la Vista JSON para la configuración. Debería ser similar al siguiente JSON:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

]

Después de habilitar el selector para el registro de seguimiento, diríjase a la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>. Puede descargar los eventos de datos del bucket de S3 que haya elegido al configurar los registros de CloudTrail.

Ejemplo: entradas de archivos de registro de GuardDuty

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra el evento del plano de datos.

```
{
  "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-EXAMPLEebbbb",
    "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"
    }
  }
}

```

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `CreateIPThreatIntelSet` (evento del plano de control).

```

{
  "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"
}

```

A partir de la información de este evento, puede determinar que la solicitud se hizo para crear una lista de amenazas de Example en GuardDuty. También puede ver que la solicitud la hizo una usuaria llamada Alice el 14 de junio de 2018.

Identity and Access Management para Amazon GuardDuty

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los gestionadores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede estar autenticado (iniciar sesión) y autorizado (tener permisos) para utilizar recursos de GuardDuty. IAM es un servicio de Servicio de AWS que se puedes utilizar sin cargo adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Amazon GuardDuty con IAM](#)
- [Ejemplos de políticas basadas en identidades de Amazon GuardDuty](#)
- [Uso de roles vinculados a servicios para Amazon GuardDuty](#)
- [Políticas administradas por AWS para Amazon GuardDuty](#)
- [Solución de problemas de identidad y acceso de Amazon GuardDuty](#)

Público

La forma en que utiliza AWS Identity and Access Management (IAM) varía en función del rol:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Solución de problemas de identidad y acceso de Amazon GuardDuty](#))
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo funciona Amazon GuardDuty con IAM](#))
- Administrador de IAM: escriba políticas para administrar el acceso (consulte [Ejemplos de políticas basadas en identidades de Amazon GuardDuty](#))

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado como Usuario raíz de la cuenta de AWS, un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de un origen de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las

credenciales de Google/Facebook. Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In.

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

Usuario raíz de la Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión llamada Cuenta de AWS del usuario raíz que tiene acceso completo a todos los Servicios de AWS y recursos. Recomendamos encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS con credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, proveedor de identidades web o Directory Service que accede a Servicios de AWS mediante credenciales de un origen de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte [Solicitar que los usuarios humanos utilicen la federación con un proveedor de identidades para acceder a AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un usuario a un rol de IAM \(consola\)](#) o llamando a una operación de la API de la AWS CLI o AWS. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política define permisos cuando se asocia con una identidad o recurso. AWS evalúa estas políticas cuando una entidad principal realiza una solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

Mediante políticas, los administradores especifican quién tiene acceso a qué definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a los roles, que luego los usuarios pueden asumir. Las políticas de IAM definen permisos independientemente del método utilizado para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos JSON de políticas de permisos que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en la identidad pueden ser políticas integradas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe [especificar una entidad principal](#) en una política en función de recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer el máximo de permisos concedidos por los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en la identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): establecen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCP\)](#) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte [Lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo funciona Amazon GuardDuty con IAM

Antes de utilizar IAM para administrar el acceso a GuardDuty, conozca qué características de IAM se pueden utilizar con GuardDuty.

Características de IAM que se pueden utilizar con Amazon GuardDuty

Característica de IAM	Compatibilidad con GuardDuty
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener información general sobre cómo funcionan GuardDuty y otros servicios de AWS con la mayoría de las características de IAM, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Políticas basadas en identidades para GuardDuty

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de las políticas de JSON de IAM](#) en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de GuardDuty

Para ver ejemplos de políticas basadas en identidades de GuardDuty, consulte [Ejemplos de políticas basadas en identidades de Amazon GuardDuty](#).

Políticas basadas en recursos de GuardDuty

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Acciones de políticas para GuardDuty

Compatibilidad con las acciones de políticas: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de GuardDuty, consulte [Acciones definidas por Amazon GuardDuty](#) en la Referencia de autorizaciones de servicio.

Las acciones de políticas de GuardDuty utilizan el siguiente prefijo antes de la acción:

```
guardduty
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
    "guardduty:action1",  
    "guardduty:action2"  
]
```

Para ver ejemplos de políticas basadas en identidades de GuardDuty, consulte [Ejemplos de políticas basadas en identidades de Amazon GuardDuty](#).

Recursos de políticas para GuardDuty

Compatibilidad con los recursos de políticas: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Para las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de GuardDuty y sus ARN, consulte [Recursos definidos por Amazon GuardDuty](#) en la Referencia de autorizaciones de servicio. Para obtener información sobre

las acciones con las que puede especificar el ARN de cada recurso, consulte [Acciones definidas por Amazon GuardDuty](#).

Para ver ejemplos de políticas basadas en identidades de GuardDuty, consulte [Ejemplos de políticas basadas en identidades de Amazon GuardDuty](#).

Claves de condición de política para GuardDuty

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puedes crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de GuardDuty, consulte [Claves de condición de Amazon GuardDuty](#) en la Referencia de autorizaciones de servicio. Para obtener más información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte [Acciones definidas por Amazon GuardDuty](#).

Para ver ejemplos de políticas basadas en identidades de GuardDuty, consulte [Ejemplos de políticas basadas en identidades de Amazon GuardDuty](#).

Listas de control de acceso (ACL) de GuardDuty

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con GuardDuty

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede asociar etiquetas a entidades de

IAM y recursos de AWS y, a continuación, diseñar políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte [Definición de permisos con la autorización de ABAC](#) en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del usuario de IAM.

Uso de credenciales temporales con GuardDuty

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a corto plazo a los recursos de AWS y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda que genere de forma dinámica credenciales temporales en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#) y [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Permisos de entidades principales entre servicios para GuardDuty

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

Roles de servicio para GuardDuty

Compatibilidad con roles de servicio: sí

Un rol de servicio es un [rol de IAM](#) que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener

más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

 Warning

Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de GuardDuty. Edite los roles de servicio solo cuando GuardDuty proporcione directrices para hacerlo.

Roles vinculados a servicios para GuardDuty

Admite roles vinculados a servicios: sí

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de GuardDuty, consulte [Uso de roles vinculados a servicios para Amazon GuardDuty](#).

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta [Servicios de AWS que funcionan con IAM](#). Busque un servicio en la tabla que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de Amazon GuardDuty

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de GuardDuty. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por GuardDuty, incluido el formato de los ARN para cada tipo de recurso, consulte [Acciones, recursos y claves de condición para Amazon GuardDuty](#) en la Referencia de autorizaciones de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola de GuardDuty](#)
- [Permisos necesarios para habilitar GuardDuty](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)
- [Política de IAM personalizada para conceder acceso de solo lectura a GuardDuty](#)
- [Denegación de acceso a los resultados de GuardDuty](#)
- [Uso de una política de IAM personalizada para limitar el acceso a los recursos de GuardDuty](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear o eliminar los recursos de GuardDuty de la cuenta, así como acceder a ellos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comienza con las políticas administradas por AWS y continúa con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de tarea, utiliza las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas gestionadas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesite usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para obtener una mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de la consola de GuardDuty

Para acceder a la consola de Amazon GuardDuty, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y consultar los detalles de los recursos de GuardDuty en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la consola de GuardDuty, adjunte también a las entidades la política administrada por AWS `ConsoleAccess` o `ReadOnly`. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM:

Permisos necesarios para habilitar GuardDuty

Para conceder permisos que deben tener varias identidades de IAM (usuarios, grupos y roles), adjunte la política [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#) necesaria para habilitar GuardDuty.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
    }
  ]
}
```

Política de IAM personalizada para conceder acceso de solo lectura a GuardDuty

Para conceder acceso de solo lectura a GuardDuty, puede utilizar la política administrada `AmazonGuardDutyReadOnlyAccess`.

Para crear una política personalizada que conceda a un rol de IAM, usuario o grupo acceso de solo lectura a GuardDuty, puede usar la siguiente declaración:

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": "*"
    }
  ]
}
```

Denegación de acceso a los resultados de GuardDuty

Puede usar la siguiente política para denegar a un rol de IAM, usuario o grupo acceso a los resultados de GuardDuty. Los usuarios no pueden ver los resultados ni los detalles de los resultados, pero pueden acceder al resto de operaciones de GuardDuty:

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"
}
]
}

```

Uso de una política de IAM personalizada para limitar el acceso a los recursos de GuardDuty

Para definir el acceso de un usuario a GuardDuty en función del ID de detector, puede utilizar todas las [acciones de la API de GuardDuty](#) en sus políticas de IAM personalizadas, excepto las siguientes operaciones:

- guardduty:CreateDetector

- `guardduty:DeclineInvitations`
- `guardduty>DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Utilice las siguientes operaciones en una política de IAM para definir el acceso de un usuario a GuardDuty según los ID de IPSet y de ThreatIntelSet:

- `guardduty>DeleteIPSet`
- `guardduty>DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

En los siguientes ejemplos se muestra cómo crear políticas con algunas de las operaciones anteriores:

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateDetector`, con el ID de detector 1234567 en la región us-east-1:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
    }
  ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con el ID de detector 1234567 y el ID de IPSet 000000 en la región us-east-1:

 Note

Asegúrese de que el usuario tiene los permisos necesarios para acceder a las listas de IP de confianza y a las listas de amenazas en GuardDuty. Para obtener más información, consulte [Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/ipset/000000"
    }
  ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con cualquier ID de detector y el ID de IPSet 000000 en la región us-east-1:

 Note

Asegúrese de que el usuario tiene los permisos necesarios para acceder a las listas de IP de confianza y a las listas de amenazas en GuardDuty. Para obtener más información, consulte [Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/ipset/000000"
    }
  ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con su ID de detector y cualquier ID de IPSet en la región us-east-1:

 Note

Asegúrese de que el usuario tiene los permisos necesarios para acceder a las listas de IP de confianza y a las listas de amenazas en GuardDuty. Para obtener más información, consulte [Configurar los requisitos previos para las listas de entidades y las listas de direcciones IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/ipset/*"
    }
  ]
}
```



```
}  
]  
}
```

Uso de roles vinculados a servicios para Amazon GuardDuty

Amazon GuardDuty utiliza [roles vinculados a servicios](#) de AWS Identity and Access Management (IAM). Un rol vinculado a servicios (SLR) es un tipo único de rol de IAM que está vinculado directamente a GuardDuty. Los roles vinculados a servicios están predefinidos por GuardDuty e incluyen todos los permisos que GuardDuty necesita para llamar a otros servicios de AWS en su nombre.

Con un rol vinculado a servicios, puede configurar GuardDuty sin agregar los permisos necesarios manualmente. GuardDuty define los permisos de su rol vinculado a servicios y, a menos que los permisos estén definidos de otra manera, solo GuardDuty puede asumir el rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

GuardDuty admite el uso de roles vinculados a servicios en todas las regiones en las que GuardDuty está disponible. Para obtener más información, consulte [Regiones y puntos de conexión](#).

Puede eliminar el rol vinculado a servicios de GuardDuty solo después de deshabilitar primero GuardDuty en todas las regiones en las que se ha habilitado. De esta forma se protegen los recursos de GuardDuty, ya que evita que se pueda eliminar accidentalmente el permiso de acceso a estos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM y busque los servicios que tienen Sí en la columna Rol vinculado a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios de GuardDuty

GuardDuty usa el rol vinculado a servicios (SLR) denominado `AWSServiceRoleForAmazonGuardDuty`. El SLR permite a GuardDuty llevar a cabo las siguientes tareas. También permite a GuardDuty incluir los metadatos recuperados que pertenecen a la instancia de EC2 en los resultado que GuardDuty pueda generar sobre la posible amenaza. El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDuty` confía en el servicio `guardduty.amazonaws.com` para asumir el rol.

Las políticas de permisos ayudan a GuardDuty a realizar las siguientes tareas:

- Utilice las acciones de Amazon EC2 para administrar y recuperar información sobre las instancias de EC2, imágenes y componentes de red, como VPC, subredes y puertas de enlace de tránsito.
- Utilice acciones de AWS Systems Manager para administrar asociaciones de SSM en instancias de Amazon EC2 cuando habilite la Supervisión en tiempo de ejecución de GuardDuty con el agente automatizado para Amazon EC2. Cuando la configuración automatizada del agente de GuardDuty está desactivada, GuardDuty solo considera aquellas instancias de EC2 que tienen una etiqueta de inclusión (`GuardDutyManaged:true`).
- Utilice acciones AWS Organizations para describir las cuentas asociadas y el ID de la organización.
- Utilice las acciones de Amazon S3 para recuperar información sobre buckets y objetos de S3.
- Utilice las acciones de AWS Lambda para recuperar información sobre las funciones de Lambda y las etiquetas.
- Utilice las acciones de Amazon EKS para administrar y recuperar información sobre los clústeres de EKS y administrar los [complementos de Amazon EKS](#) en los clústeres de EKS. Las acciones de EKS también recuperan la información sobre las etiquetas asociadas a GuardDuty.
- Utilice IAM para crear el [Permisos de rol vinculado al servicio para Malware Protection for EC2](#) después de que se haya habilitado Malware Protection for EC2.
- Utilice las acciones de Amazon ECS para administrar y recuperar información sobre los clústeres de Amazon ECS y administrar la configuración de la cuenta de Amazon ECS con `guarddutyActivate`. Las acciones que pertenecen a Amazon ECS también recuperan la información sobre las etiquetas asociadas a GuardDuty.

El rol se configura con la siguiente [política administrada por AWS](#), que se denomina `AmazonGuardDutyServiceRolePolicy`.

Para ver los permisos de esta política, consulte [AmazonGuardDutyServiceRolePolicy](#) en la Guía de referencia de políticas administradas por AWS.

A continuación se presenta la política de confianza que se asocia al rol vinculado a servicio `AWSServiceRoleForAmazonGuardDuty`:

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
```

Para obtener más información sobre actualizaciones a la política AmazonGuardDutyServiceRolePolicy, consulte [Actualizaciones de GuardDuty en las políticas administradas por AWS](#). Para obtener alertas automáticas sobre cambios en esta política, suscríbase a la fuente RSS en la página de [Historial de revisión](#).

Creación de un rol vinculado a servicios de GuardDuty

El rol vinculado a servicios AWSServiceRoleForAmazonGuardDuty se crea automáticamente cuando se habilita GuardDuty por primera vez o al habilitar GuardDuty en una región compatible en la que no estaba habilitado. También puede crear el rol vinculado al servicio manualmente con la consola de IAM, la AWS CLI o la API de IAM.

Important

El rol vinculado a servicios creado para la cuenta de administrador delegado de GuardDuty no se aplica a cuentas de GuardDuty de miembros.

Debe configurar permisos para permitir a una entidad principal de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol vinculado a servicios AWSServiceRoleForAmazonGuardDuty se cree correctamente, la entidad principal de IAM con la que se utiliza GuardDuty debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a un usuario, un grupo o un rol de :

 Note

Sustituya el *ID de cuenta* de ejemplo del siguiente ejemplo por su ID de Cuenta de AWS real.

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"
    }
  ]
}
```

```
}
```

Para obtener más información sobre cómo crear un rol manualmente, consulte [Crear un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Edición de un rol vinculado a servicios de GuardDuty

GuardDuty no le permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDuty`. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios de GuardDuty

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

Important

Si ha habilitado Malware Protection for EC2, la eliminación de `AWSServiceRoleForAmazonGuardDuty` no elimina `AWSServiceRoleForAmazonGuardDutyMalwareProtection` automáticamente. Si desea eliminar `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulte [Eliminar un rol vinculado al servicio para Malware Protection for EC2](#).

Para poder eliminar `AWSServiceRoleForAmazonGuardDuty`, primero debe deshabilitar GuardDuty en todas las regiones en las que esté habilitado. Si el servicio GuardDuty está habilitado cuando intente eliminar el rol vinculado a servicios, no se eliminará. Para obtener más información, consulte [Suspensión o deshabilitación de GuardDuty](#).

Al deshabilitar GuardDuty, `AWSServiceRoleForAmazonGuardDuty` no se elimina automáticamente. Si vuelve a habilitar GuardDuty, se iniciará con el `AWSServiceRoleForAmazonGuardDuty` existente.

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de IAM para eliminar el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDuty`. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones de AWS admitidas

Amazon GuardDuty admite el uso del rol vinculado a servicios `AWSServiceRoleForAmazonGuardDuty` en todas las Regiones de AWS en las que GuardDuty está disponible. Para obtener una lista de las regiones en las que GuardDuty está disponible actualmente, consulte [Amazon GuardDuty endpoints and quotas](#) en la Referencia general de Amazon Web Services.

Permisos de rol vinculado al servicio para Malware Protection for EC2

Malware Protection for EC2 utiliza el rol vinculado al servicio (SLR) denominado `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Este SLR permite a Malware Protection for EC2 llevar a cabo análisis sin agentes para detectar malware en la cuenta de GuardDuty. Permite a GuardDuty crear una instantánea del volumen de EBS en su cuenta y compartirla con la cuenta de servicio de GuardDuty. Una vez que GuardDuty evalúa la instantánea, incluye los metadatos recuperados de la carga de trabajo del contenedor y la instancia de EC2 en los resultados de Malware Protection for EC2. El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` confía en el servicio `malware-protection.guarddduty.amazonaws.com` para asumir el rol.

Las políticas de permisos de este rol ayudan a Malware Protection for EC2 a realizar las siguientes tareas:

- Utilice las acciones de Amazon Elastic Compute Cloud (Amazon EC2) para recuperar información sobre las instancias de Amazon EC2, los volúmenes y las instantáneas. Malware Protection for EC2 también concede permiso para acceder a los metadatos de clúster de Amazon EKS y Amazon ECS.
- Crear instantáneas para los volúmenes de EBS cuya etiqueta `GuardDutyExcluded` no esté configurada como `true`. De forma predeterminada, las instantáneas se crean con una etiqueta `GuardDutyScanId`. No elimine esta etiqueta. Si lo hace, Malware Protection for EC2 no tendrá acceso a las instantáneas.

 Important

Si establece `GuardDutyExcluded` en `true`, el servicio GuardDuty no podrá acceder a estas instantáneas en el futuro. Esto se debe a que las demás declaraciones de este rol vinculado a servicios impiden que GuardDuty lleve a cabo cualquier acción en las instantáneas que tienen el valor de `GuardDutyExcluded` establecido en `true`.

- Permitir compartir y eliminar instantáneas solo si la etiqueta `GuardDutyScanId` existe y la etiqueta `GuardDutyExcluded` no está establecida en `true`.

 Note

No permite que Malware Protection for EC2 haga públicas las instantáneas.

- Acceder a las claves administradas por el cliente, excepto a las que tengan una etiqueta `GuardDutyExcluded` establecida en `true`, para llamar a `CreateGrant` a fin de crear un volumen de EBS cifrado, y acceder a él, a partir de la instantánea cifrada que se comparte con la cuenta de servicio de GuardDuty. Para obtener una lista de las cuentas de servicio de GuardDuty de cada región, consulte [Cuentas de servicio de GuardDuty por Región de AWS](#).
- Acceda a los registros de CloudWatch de los clientes para crear el grupo de registro de Malware Protection for EC2, así como para colocar los registros de eventos de análisis de malware en el grupo de registro de `/aws/guardduty/malware-scan-events`.
- Permitir que el cliente decida si quiere conservar en su cuenta las instantáneas en las que se detectó el malware. Si el análisis detecta malware, el rol vinculado a servicios permite a GuardDuty agregar dos etiquetas a las instantáneas: `GuardDutyFindingDetected` y `GuardDutyExcluded`.

 Note

La etiqueta `GuardDutyFindingDetected` especifica que las instantáneas contienen malware.

- Determinar si un volumen está cifrado con una clave administrada por EBS. GuardDuty lleva a cabo la acción `DescribeKey` para determinar el valor de `key Id` de la clave administrada por EBS en su cuenta.

- Obtenga la instantánea de los volúmenes EBS cifrados mediante Clave administrada de AWS, de la Cuenta de AWS y cópiela en la [Cuentas de servicio de GuardDuty](#). Para ello, utilizamos los permisos `GetSnapshotBlock` y `ListSnapshotBlocks`. GuardDuty analizará entonces la instantánea en la cuenta de servicio. Actualmente, es posible que Malware Protection for EC2 no admita el análisis de volúmenes de EBS cifrados con Clave administrada de AWS en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de características específicas por región](#).
- Permita que Amazon EC2 llame a AWS KMS en nombre de Malware Protection for EC2 para realizar varias acciones criptográficas en claves administradas por el cliente. Acciones como `kms:ReEncryptTo` y `kms:ReEncryptFrom` son obligatorias para compartir las instantáneas cifradas con las claves administradas por el cliente. Solo se puede acceder a las claves para las que la etiqueta `GuardDutyExcluded` no esté establecida en `true`.

El rol se configura con la siguiente [política administrada por AWS](#), que se denomina `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Para ver los permisos de esta política, consulte [AmazonGuardDutyMalwareProtectionServiceRolePolicy](#) en la Guía de referencia de políticas administradas de AWS.

La siguiente política de confianza se ha adjuntado al rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```


Crear un rol vinculado al servicio para Malware Protection for EC2

El rol vinculado al servicio `AWSServiceRoleForAmazonGuardDutyMalwareProtection` se crea automáticamente cuando se habilita Malware Protection for EC2 por primera vez o al habilitar Malware Protection for EC2 en una región compatible en la que no estaba habilitado. También puede crear el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente con la consola de IAM, la CLI de IAM o la API de IAM.

Note

De forma predeterminada, si es la primera vez que utiliza Amazon GuardDuty, Malware Protection for EC2 se habilita automáticamente.

Important

El rol vinculado al servicio creado para la cuenta de administrador delegado de GuardDuty no se aplica a cuentas de GuardDuty de miembro.

Debe configurar permisos para permitir a una entidad principal de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` se cree correctamente, la identidad de IAM con la que se usa GuardDuty debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a un usuario, un grupo o un rol de :

JSON

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

```

        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": [
                    "malware-protection.guarddduty.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"
    }
]
}

```

Para obtener más información sobre cómo crear un rol manualmente, consulte [Crear un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Editar un rol vinculado al servicio para Malware Protection for EC2

Malware Protection for EC2 no permite editar el rol vinculado al servicio `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminar un rol vinculado al servicio para Malware Protection for EC2

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

Important

Para poder eliminar `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, primero debe desactivar Malware Protection for EC2 en todas las regiones en las que esté habilitada.

Si Malware Protection for EC2 está habilitada al intentar eliminar el rol vinculado al servicio, el rol no se eliminará. Asegúrese de desactivar primero Malware Protection for EC2 en la cuenta.

Si selecciona Desactivar para detener el servicio de Malware Protection for EC2, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` no se elimina automáticamente. Si, a continuación, selecciona Habilitar para volver a iniciar el servicio de Malware Protection for EC2, GuardDuty empezará a utilizar el `AWSServiceRoleForAmazonGuardDutyMalwareProtection` existente.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de IAM para eliminar el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones de AWS admitidas

Amazon GuardDuty admite el uso del rol vinculado al servicio de `AWSServiceRoleForAmazonGuardDutyMalwareProtection` en todas las Regiones de AWS en las que Malware Protection for EC2 está disponible.

Para obtener una lista de las regiones en las que GuardDuty está disponible actualmente, consulte [Amazon GuardDuty endpoints and quotas](#) en la Referencia general de Amazon Web Services.

 Note

Malware Protection for EC2 no está disponible actualmente en AWS GovCloud (Este de EE. UU.) ni AWS GovCloud (Oeste de EE. UU.).

Políticas administradas por AWS para Amazon GuardDuty

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para [crear políticas administradas por el cliente de IAM](#) que le brinden a su equipo solo los permisos necesarios. Para comenzar rápidamente, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información acerca de las políticas administradas de AWS, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos en las políticas gestionadas de AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada de AWS `ReadOnlyAccess` proporciona acceso de solo lectura a todos los servicios y los recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

El elemento de la política `Version` especifica las reglas de sintaxis del lenguaje que se van a utilizar para procesar esta política. Las siguientes políticas incluyen la versión actual que IAM admite. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Versión](#).

Política administrada de AWS: AmazonGuardDutyFullAccess_v2 (recomendada)

Puede adjuntar la política AmazonGuardDutyFullAccess_v2 a las identidades de IAM. Esta política concederá a un usuario acceso completo para realizar todas las acciones de GuardDuty y acceder a los recursos necesarios. Entre AmazonGuardDutyFullAccess_v2 y AmazonGuardDutyFullAccess, GuardDuty recomienda adjuntar AmazonGuardDutyFullAccess_v2 porque ofrece una mayor seguridad y restringe las acciones administrativas a las entidades principales de servicio de GuardDuty.

Detalles del permiso

La política AmazonGuardDutyFullAccess_v2 incluye los siguientes permisos:

- GuardDuty: concede a los usuarios acceso completo a todas las acciones de GuardDuty.
- IAM:
 - Permite a los usuarios crear el rol vinculado al servicio de GuardDuty.
 - Permite ver y gestionar los roles de IAM y sus políticas para GuardDuty.
 - Permite a los usuarios transmitir un rol a GuardDuty que utiliza este rol para habilitar la característica de protección contra malware para S3 de GuardDuty. Esto es independiente de cómo se habilite la protección contra malware para S3, ya sea como parte del servicio de GuardDuty o de forma independiente.
 - El permiso para llevar a cabo una acción `iam:GetRole` en `AWSServiceRoleForAmazonGuardDutyMalwareProtection` establece si el rol vinculado al servicio (SLR) para Malware Protection for EC2 existe en una cuenta.
- Organizations:
 - Permita a los usuarios leer (ver) la estructura organizativa y las cuentas de GuardDuty.
 - Permite a los usuarios designar un administrador delegado y administrar los miembros de una organización de GuardDuty.

Para ver los permisos de esta política, consulte [AmazonGuardDutyFullAccess_v2](#) en la Guía de referencia de políticas administradas de AWS.

AWS Política administrada por: AmazonGuardDutyFullAccess

Puede adjuntar la política AmazonGuardDutyFullAccess a las identidades de IAM.

 Important

Para mejorar la seguridad y restringir los permisos a las entidades principales del servicio GuardDuty, se recomienda que utilice [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#).

Esta política concede permisos administrativos que permiten a un usuario acceso completo para realizar todas las acciones y los recursos de GuardDuty.

Detalles del permiso

Esta política incluye los siguientes permisos.

- GuardDuty: concede a los usuarios acceso completo a todas las acciones de GuardDuty.
- IAM:
 - Permite a los usuarios crear el rol vinculado al servicio de GuardDuty.
 - Permite que una cuenta de administrador habilite GuardDuty para cuentas de miembro.
 - Permite a los usuarios transmitir un rol a GuardDuty que utiliza este rol para habilitar la característica de protección contra malware para S3 de GuardDuty. Esto es independiente de cómo se habilite la protección contra malware para S3, ya sea como parte del servicio de GuardDuty o de forma independiente.
- Organizations: permite a los usuarios designar un administrador delegado y administrar los miembros de una organización de GuardDuty.

El permiso para llevar a cabo una acción `iam:GetRole` en `AWSServiceRoleForAmazonGuardDutyMalwareProtection` establece si el rol vinculado al servicio (SLR) para Malware Protection for EC2 existe en una cuenta.

Para ver los permisos de esta política, consulte [AmazonGuardDutyFullAccess](#) en la Guía de referencia de políticas administradas por AWS.

AWS Política administrada por: AmazonGuardDutyReadOnlyAccess

Puede adjuntar la política `AmazonGuardDutyReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura para que un usuario pueda ver los resultados de GuardDuty y los detalles de su organización de GuardDuty.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- **GuardDuty**: permite a los usuarios ver los resultados de GuardDuty y llevar a cabo operaciones de la API que comiencen por `Get`, `List` o `Describe`.
- **Organizations**: permite a los usuarios recuperar información sobre la configuración de su organización de GuardDuty, incluidos los detalles de la cuenta de administrador delegado.

Para ver los permisos de esta política, consulte [AmazonGuardDutyReadOnlyAccess](#) en la Guía de referencia de políticas administradas por AWS.

AWS Política administrada de: AmazonGuardDutyServiceRolePolicy

No puede adjuntar AmazonGuardDutyServiceRolePolicy a sus entidades de IAM. Esta política administrada por AWS está adjunta a un rol vinculado a servicios que permite a GuardDuty llevar a cabo acciones en su nombre. Para obtener más información, consulte [Permisos de roles vinculados a servicios de GuardDuty](#).

Actualizaciones de GuardDuty en las políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para GuardDuty debido a que este servicio comenzó a hacer un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de GuardDuty.

Cambio	Descripción	Fecha
AmazonGuardDutyFullAccess_v2 – agregó una nueva política.	Se agregó una nueva política AmazonGuardDutyFullAccess_v2. Esto se recomienda porque sus permisos mejoran la seguridad	04 de junio de 2025

Cambio	Descripción	Fecha
	al restringir las acciones administrativas a las entidades principales de servicio de GuardDuty en función de los roles y las políticas de IAM y de la integración de AWS Organizations.	
AmazonGuardDutyServiceRolePolicy : actualización de una política existente	Se agregó el permiso <code>ec2:DescribeVpcs</code> . Esto permite que GuardDuty realice un seguimiento de las actualizaciones de la VPC, como recuperar el CIDR de la VPC.	22 de agosto de 2024

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy : actualización de una política existente	Permiso agregado que permite transmitir un rol de IAM a GuardDuty al habilitar la protección contra malware para S3. <pre>{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } } }</pre>	10 de junio de 2024

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy : actualización de una política existente.	Utilice acciones de AWS Systems Manager para administrar asociaciones de SSM en instancias de Amazon EC2 cuando habilite la Supervisión en tiempo de ejecución de GuardDuty con el agente automatizado para Amazon EC2. Cuando la configuración automatizada del agente de GuardDuty está desactivada, GuardDuty solo considera aquellas instancias de EC2 que tienen una etiqueta de inclusión (GuardDuty Managed :true).	26 de marzo de 2024
AmazonGuardDutyServiceRolePolicy : actualización de una política existente.	GuardDuty ha agregado un nuevo permiso: <code>organization:DescribeOrganization</code> para recuperar el ID de organización de la cuenta de la Amazon VPC compartida y establecer la política de punto de conexión de Amazon VPC con el ID de organización.	9 de febrero de 2024

Cambio	Descripción	Fecha
AmazonGuardDutyMalwareProtectionServiceRolePolicy : actualización de una política existente.	Malware Protection for EC2 ha agregado dos permisos: <code>GetSnapshotBlock</code> y <code>ListSnapshotBlocks</code> para obtener la instantánea de un volumen de EBS (cifrado mediante Clave administrada de AWS) de la Cuenta de AWS y copiarlo en la cuenta de servicio de GuardDuty antes de iniciar el análisis de malware.	25 de enero de 2024
AmazonGuardDutyServiceRolePolicy : actualización de una política existente	Se han agregado nuevos permisos para que GuardDuty pueda agregar la configuración de cuentas guardduty <code>Activate</code> de Amazon ECS y realizar operaciones de enumeración y descripción en clústeres de Amazon ECS.	26 de noviembre de 2023
AmazonGuardDutyReaadOnlyAccess – actualización de una política actual	GuardDuty agregó una nueva política para <code>organizations</code> para <code>ListAccounts</code> .	16 de noviembre de 2023
AmazonGuardDutyFullAccess – actualización de una política actual	GuardDuty agregó una nueva política para <code>organizations</code> para <code>ListAccounts</code> .	16 de noviembre de 2023

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy – actualización de una política actual	GuardDuty agregó nuevos permisos para admitir la próxima característica de supervisión en tiempo de ejecución de EKS en GuardDuty.	8 de marzo de 2023
AmazonGuardDutyServiceRolePolicy : actualización de una política existente	GuardDuty agregó nuevos permisos para permitir a GuardDuty crear un rol vinculado al servicio para Malware Protection for EC2. Esto ayudará a GuardDuty a agilizar el proceso de habilitación de Malware Protection for EC2. GuardDuty ahora puede llevar a cabo la siguiente acción de IAM: <pre>{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }</pre>	21 de febrero de 2023

Cambio	Descripción	Fecha
AmazonGuardDutyFullAccess – actualización de una política actual	GuardDuty actualizó el ARN de <code>iam:GetRole</code> a <code>*AWSServiceRoleForAmazonGuardDutyMalwareProtection</code> .	26 de julio de 2022
AmazonGuardDutyFullAccess – actualización de una política actual	GuardDuty agregó un nuevo <code>AWSServiceName</code> para permitir la creación de un rol vinculado al servicio mediante <code>iam:CreateServiceLinkedRole</code> para el servicio de Malware Protection for EC2 de GuardDuty. GuardDuty ahora puede llevar a cabo la acción <code>iam:GetRole</code> para obtener información de <code>AWSServiceRole</code>.	26 de julio de 2022

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy – actualización de una política actual	GuardDuty agregó nuevos permisos para permitir que GuardDuty utilice las acciones de red de Amazon EC2 para mejorar los resultados. GuardDuty ahora puede llevar a cabo las siguientes acciones de EC2 para obtener información sobre cómo se comunican sus instancias de EC2. Esta información se utiliza para mejorar la precisión de los resultados. • <code>ec2:DescribeVpcEndpoints</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:DescribeVpcPeeringConnections</code> • <code>ec2:DescribeTransitGatewayAttachments</code>	3 de agosto de 2021
GuardDuty comenzó a hacer un seguimiento de los cambios	GuardDuty comenzó a hacer un seguimiento de los cambios de las políticas administradas por AWS.	3 de agosto de 2021

Solución de problemas de identidad y acceso de Amazon GuardDuty

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir al trabajar con GuardDuty e IAM.

Temas

- [No estoy autorizado a llevar a cabo una acción en GuardDuty](#)
- [No estoy autorizado a llevar a cabo iam:PassRole.](#)
- [Quiero permitir que personas externas a mi Cuenta de AWS accedan a mis recursos de GuardDuty.](#)

No estoy autorizado a llevar a cabo una acción en GuardDuty

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM mateojackson intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *my-example-widget*, pero no tiene los permisos ficticios guardduty: *GetWidget*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
guardduty:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario mateojackson debe actualizarse para permitir el acceso al recurso *my-example-widget* mediante la acción guardduty: *GetWidget*.

Si necesita ayuda, póngase en contacto con su gestor de AWS. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a llevar a cabo iam:PassRole.

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción iam:PassRole, se deben actualizar las políticas a fin de permitirle pasar un rol a GuardDuty.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado marymajor intenta utilizar la consola para llevar a cabo una acción en GuardDuty. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su gestor de AWS. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas externas a mi Cuenta de AWS accedan a mis recursos de GuardDuty.

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre si GuardDuty admite estas características, consulte [Cómo funciona Amazon GuardDuty con IAM](#).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Acceso para un usuario de IAM en otra Cuenta de AWS propia](#) en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulta [Proporcionar acceso a Cuentas de AWS que son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Validación de la conformidad de Amazon GuardDuty

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte [Servicios de AWS incluidos por programa de conformidad](#) y escoja el programa de conformidad que le interese. Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puedes descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. Para obtener más información sobre la responsabilidad de conformidad al usar Servicios de AWS, consulte la [Documentación de seguridad de AWS](#).

Resiliencia de Amazon GuardDuty

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulta [Infraestructura global de AWS](#).

Seguridad de la infraestructura en Amazon GuardDuty

Como se trata de un servicio administrado, Amazon GuardDuty se encuentra protegido por la seguridad de la red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte [Seguridad en la nube de AWS](#). Para diseñar su entorno de AWS siguiendo las prácticas recomendadas de seguridad de infraestructura, consulte [Protección de la infraestructura](#) en Portal de seguridad de AWS Well-Architected Framework.

Utilice llamadas a la API publicadas en AWS para acceder a GuardDuty a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Amazon GuardDuty y puntos de conexión de VPC de interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre la VPC y Amazon GuardDuty mediante la creación de un punto de conexión de VPC de interfaz. Los puntos de conexión de interfaz cuentan con tecnología de [AWS PrivateLink](#), que permite acceder de forma privada a las API de GuardDuty sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para establecer comunicación con las API de GuardDuty. El tráfico entre la VPC y GuardDuty no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más [interfaces de red elásticas](#) en las subredes.

Para obtener más información, consulte [Puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#) en la Guía de AWS PrivateLink.

Consideraciones sobre los puntos de conexión de VPC de GuardDuty

Antes de configurar un punto de conexión de VPC de interfaz para GuardDuty, revise [Propiedades y limitaciones de los puntos de conexión de interfaz](#) en la Guía de AWS PrivateLink.

GuardDuty admite realizar llamadas a todas las acciones de la API desde la VPC.

Crear un punto de conexión de VPC de interfaz para GuardDuty

Puede crear un punto de conexión de VPC para el servicio de GuardDuty mediante la consola de Amazon VPC o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink.

Cree un punto de conexión de VPC para GuardDuty mediante el siguiente nombre de servicio:

- `com.amazonaws.region.guardduty`
- `com.amazonaws.region.guardduty-fips` (punto de conexión de FIPS)

Si habilita el DNS privado para el punto de conexión, puede realizar solicitudes de API a GuardDuty mediante el nombre de DNS predeterminado para la región, por ejemplo, `guardduty.us-east-1.amazonaws.com`.

Para obtener más información, consulte [Acceso a un servicio a través de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink.

Crear una política de punto de conexión de VPC para GuardDuty

Puede asociar una política de punto de conexión al punto de conexión de VPC que controla el acceso a GuardDuty. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte [Control del acceso a los servicios con puntos de conexión de VPC](#) en la Guía de AWS PrivateLink.

Ejemplo: política de punto de conexión de VPC para acciones de GuardDuty

A continuación, se muestra un ejemplo de una política de punto de conexión para GuardDuty. Cuando se asocia a un punto de conexión, esta política concede acceso a las acciones de GuardDuty enumeradas para todas las entidades principales en todos los recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "guardduty:listDetectors",
        "guardduty:getDetector",
        "guardduty:getFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes

que se compartan con usted. Para obtener información sobre el uso compartido de VPC, consulte [Compartir su VPC con otras cuentas](#) en la Guía del usuario de Amazon VPC.

Integración de GuardDuty con los servicios de seguridad de AWS

GuardDuty se puede integrar en otros servicios de seguridad de AWS. Estos servicios pueden ingerir datos de GuardDuty para que pueda ver los resultados de manera diferente. Consulte las siguientes opciones de integración para obtener más información sobre cómo funciona cada servicio con GuardDuty.

Integración de GuardDuty con AWS Security Hub CSPM

AWS Security Hub CSPM recopila datos de seguridad de todas sus cuentas y servicios de AWS y de los productos de terceros compatibles para evaluar el estado de seguridad de su entorno de acuerdo con los estándares del sector y de las prácticas recomendadas. Además de evaluar su postura de seguridad, Security Hub crea una ubicación central para los resultados en todos sus servicios de AWS integrados y productos de socios de AWS. Al habilitar Security Hub con GuardDuty, Security Hub podrá ingerir automáticamente los datos de resultados de GuardDuty.

Para obtener más información sobre el uso de Security Hub con GuardDuty, consulte [Integrating with \(Integración de con AWS Security Hub CSPM\)](#).

Integración de GuardDuty con Amazon Detective

Amazon Detective utiliza los datos de registro de todas sus cuentas de AWS para crear visualizaciones de datos de los recursos y direcciones IP que interactúan con su entorno. Las visualizaciones de Detective le ayudan a investigar los problemas de seguridad de forma rápida y sencilla. Una vez que ambos servicios estén activados, puede pasar de los detalles de los resultados de GuardDuty a la información en la consola de Detective.

Para obtener más información sobre el uso de Detective con GuardDuty, consulte [Integración con Amazon Detective](#).

Integrating with (Integración de con AWS Security Hub CSPM

[AWS Security Hub CSPM](#) brinda una visión completa de su estado de seguridad en AWS y ayuda a comprobar su entorno con las prácticas recomendadas y los estándares del sector de seguridad.

Security Hub recopila datos de seguridad de todas las cuentas de AWS, de los servicios y de los productos de terceros compatibles y le ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

La integración de Amazon GuardDuty con Security Hub le permite enviar resultados de GuardDuty a Security Hub. Security Hub puede incluir esos resultados en su análisis de la posición de seguridad.

Contenido

- [Cómo envía Amazon GuardDuty los resultados a AWS Security Hub CSPM](#)
 - [Tipos de resultados que GuardDuty envía a Security Hub](#)
 - [Latencia para el envío de nuevos resultados](#)
 - [Reintento cuando Security Hub no está disponible](#)
 - [Actualización de los resultados existentes en Security Hub](#)
- [Visualización de los resultados de GuardDuty en AWS Security Hub CSPM](#)
 - [Interpretación de los nombres de resultados de GuardDuty en AWS Security Hub CSPM](#)
 - [Resultado típico de GuardDuty](#)
- [Habilitación y configuración de la integración](#)
- [Utilizar controles de GuardDuty en Security Hub](#)
- [Detención de la publicación de resultados en Security Hub](#)

Cómo envía Amazon GuardDuty los resultados a AWS Security Hub CSPM

En AWS Security Hub CSPM, los problemas de seguridad se rastrean como resultados. Algunos resultados provienen de problemas detectados por otros servicios de AWS o por socios terceros. Security Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados.

Security Hub proporciona herramientas para administrar los resultados de todas estas fuentes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Para obtener más información, consulte [Visualización de resultados](#) en la Guía del usuario de AWS Security Hub CSPM. También puede realizar un seguimiento del estado de una investigación de un resultado. Para obtener más información, consulte [Adopción de medidas en función de los resultados](#) en la Guía del usuario de AWS Security Hub CSPM.

Todos los resultados en Security Hub usan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema, los recursos

afectados y el estado actual del resultado. Consulte [Formato de resultados de seguridad de AWS \(ASFF\)](#) en la Guía del usuario de AWS Security Hub CSPM.

Amazon GuardDuty es uno de los servicios de AWS que envía resultados a Security Hub.

Tipos de resultados que GuardDuty envía a Security Hub

Cuando habilita GuardDuty y Security Hub en la misma cuenta y Región de AWS, GuardDuty comienza a enviar todos los resultados generados a Security Hub. Estos resultados se envían a Security Hub por medio del [Formato de resultados de seguridad \(ASFF\) de AWS](#). En ASFF, el campo Types proporciona el tipo de resultado.

Latencia para el envío de nuevos resultados

Cuando GuardDuty crea un nuevo resultado, generalmente se envía a Security Hub en un plazo de cinco minutos.

Reintento cuando Security Hub no está disponible

Si Security Hub no está disponible, GuardDuty vuelve a intentar enviar los resultados hasta que se reciben.

Actualización de los resultados existentes en Security Hub

Después de enviar un resultado a Security Hub, GuardDuty envía actualizaciones para reflejar observaciones adicionales de la actividad del resultado a Security Hub. Las nuevas observaciones de estos resultados se envían a Security Hub en función de la configuración de [Paso 5: Frecuencia de exportación de los resultados](#) en la Cuenta de AWS.

Cuando se archiva o desarchiva un resultado, GuardDuty no envía ese resultado a Security Hub. Los resultados desarchivados manualmente que luego se activan en GuardDuty no se envían a Security Hub.

Visualización de los resultados de GuardDuty en AWS Security Hub CSPM

Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Security Hub CSPM en <https://console.aws.amazon.com/securityhub/>.

Ahora puede utilizar cualquiera de las siguientes formas para ver los resultados de GuardDuty en la consola de Security Hub:

Opción 1: Uso de integraciones en Security Hub

1. En el panel de navegación de la izquierda, seleccione Integraciones.
2. En la página Integraciones, verifique el estado de Amazon: GuardDuty.
 - Si el estado es Aceptación de resultados, seleccione Ver resultados junto a Aceptación de resultados.
 - Si no es así, para obtener más información sobre cómo funcionan las integraciones, consulte [Integraciones de Security Hub](#) en la Guía del usuario de AWS Security Hub CSPM.

Opción 2: Uso de Resultados en Security Hub

1. En el panel de navegación izquierdo, elija Resultados.
2. En la página Resultados, agregue el filtro Nombre del producto e introduzca **GuardDuty** para ver solo los resultados de GuardDuty.

Interpretación de los nombres de resultados de GuardDuty en AWS Security Hub CSPM

GuardDuty envía los resultados a Security Hub con el [Formato de resultados de seguridad de AWS \(ASFF\)](#). En ASFF, el campo Types proporciona el tipo de resultado. Los tipos de ASFF utilizan un esquema de nomenclatura diferente al de los tipos de GuardDuty. En la siguiente tabla se detallan todos los tipos de resultados de GuardDuty con sus homólogos de ASFF tal y como aparecen en Security Hub.

Note

Para algunos tipos de resultados de GuardDuty, Security Hub asigna diferentes nombres de resultados de ASFF en función de si el valor de Rol de recurso de los detalles del resultado era ACTOR o TARGET. Para obtener más información consulte () [Detalles de los resultados](#).

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedC redentials

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
AttackSequence:S3/CompromisedData	TTPs/AttackSequence:S3/CompromisedData
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.FailedLogin

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
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:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/KernelModuleLoaded	TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded
DefenseEvasion:Runtime/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
Discovery:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:Runtime/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

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller
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

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution: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
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
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

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
Persistence:IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
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

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
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

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
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

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
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
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
<u>UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS</u>	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
<u>UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS</u>	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
<u>UnauthorizedAccess:IAMUser/MaliciousIPCaller</u>	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
<u>UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom</u>	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
<u>UnauthorizedAccess:IAMUser/TorIPCaller</u>	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
<u>UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom</u>	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
<u>UnauthorizedAccess:Lambda/TorClient</u>	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
<u>UnauthorizedAccess:Lambda/TorRelay</u>	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
<u>UnauthorizedAccess:Runtime/MetadataDNSRebind</u>	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
<u>UnauthorizedAccess:Runtime/TorRelay</u>	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
<u>UnauthorizedAccess:Runtime/TorClient</u>	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
<u>UnauthorizedAccess:S3/MaliciousIPCaller.Custom</u>	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom

Tipo de resultado de GuardDuty	Tipo de resultado de ASFF
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Resultado típico de GuardDuty

GuardDuty envía los resultados a Security Hub con el [Formato de resultados de seguridad de AWS \(ASFF\)](#).

A continuación se presenta un ejemplo de un resultado típico de GuardDuty.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
    "Unknown",
```



```

    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
"199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
"46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
"172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
"INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
"SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/
arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/
finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"

```

```
},
"Resources": [
  {
    "Type": "AwsEc2Instance",
    "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
    "Partition": "aws",
    "Region": "us-east-1",
    "Tags": {
      "Name": "kubect1"
    },
    "Details": {
      "AwsEc2Instance": {
        "Type": "t2.micro",
        "ImageId": "ami-02354e95b39ca8dec",
        "IPv4Addresses": [
          "18.234.130.16",
          "172.31.43.6"
        ],
        "VpcId": "vpc-a0c2d7c7",
        "SubnetId": "subnet-4975b475",
        "LaunchedAt": "2020-08-03T23:21:57Z"
      }
    }
  }
],
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE"
}
```

Habilitación y configuración de la integración

Para utilizar la integración con AWS Security Hub CSPM, debe habilitar Security Hub. Para obtener información acerca de cómo habilitar Security Hub, consulte la [Configuración de Security Hub](#) en la Guía del usuario de AWS Security Hub CSPM.

Cuando habilita GuardDuty y Security Hub, la integración se habilita automáticamente. GuardDuty comienza a enviar inmediatamente los resultados a Security Hub.

Utilizar controles de GuardDuty en Security Hub

AWS Security Hub CSPM utiliza controles de seguridad para evaluar los recursos de AWS y comprobar el cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Puede utilizar los controles relacionados con los recursos de GuardDuty y los planes de protección seleccionados. Para obtener más información, consulte [Controles de Amazon GuardDuty](#) en la Guía del usuario de AWS Security Hub CSPM.

Para obtener una lista de todos los controles en los servicios y recursos de AWS, consulte la [Referencia sobre los controles de Security Hub](#) en la Guía del usuario de AWS Security Hub CSPM.

Detención de la publicación de resultados en Security Hub

Para dejar de enviar resultados a Security Hub, puede utilizar la consola de Security Hub o la API.

Consulte [Disabling and enabling the flow of findings from an integration \(console\)](#) o [Disabling the flow of findings from an integration \(Security Hub API, AWS CLI\)](#) en la Guía del usuario de AWS Security Hub CSPM.

Integración con Amazon Detective

[Amazon Detective](#) le ayuda a analizar e investigar rápidamente los eventos de seguridad en una o más cuentas de AWS mediante la generación de visualizaciones de datos que representan la forma en que sus recursos se comportan e interactúan a lo largo del tiempo. Detective crea visualizaciones de los resultados de GuardDuty.

Detective recopila los detalles de resultados de todos los tipos de resultados y proporciona acceso a los perfiles de las entidades para investigar las diferentes entidades que están involucradas en el resultado. Una entidad puede ser una Cuenta de AWS, un recurso de AWS dentro de una cuenta o una dirección IP externa que ha interactuado con sus recursos. La consola de GuardDuty permite pasar a Amazon Detective desde las siguientes entidades, según el tipo de resultado: Cuenta de AWS, rol de IAM, usuario o sesión de rol, agente de usuario, usuario federado, instancia de Amazon EC2 o dirección IP.

Contenido

- [Habilitación de la integración](#)
- [Paso de un resultado de GuardDuty a Amazon Detective](#)
- [Uso de la integración con un entorno multicuenta de GuardDuty](#)

Habilitación de la integración

Para utilizar Amazon Detective con GuardDuty, primero debe habilitar Amazon Detective. Para más información sobre cómo habilitar Detective, consulte [Primeros pasos con Amazon Detective](#) en la Guía de administración de Amazon Detective.

Cuando habilita GuardDuty y Detective, la integración se activa automáticamente. Una vez activado, Detective recopilará inmediatamente los datos de los resultados de GuardDuty.

Note

GuardDuty envía los resultados a Detective en función de la frecuencia de exportación de los resultados de GuardDuty. De forma predeterminada, la frecuencia de exportación de las actualizaciones de los resultados existentes es de 6 horas. Para garantizar que Detective reciba las actualizaciones más recientes de sus resultados, se recomienda que cambie la frecuencia de exportación a 15 minutos en cada región en la que utilice Detective con GuardDuty. Para obtener más información consulte () [Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados](#).

Paso de un resultado de GuardDuty a Amazon Detective

1. Inicie sesión en la consola <https://console.aws.amazon.com/guardduty/>.
2. Elija un único resultado de la tabla de resultados.
3. Seleccione Investigar con Detective en el panel de detalles de los resultados.
4. Elija un aspecto del resultado para investigarlo con Amazon Detective. Esto abre la consola de Detective para ese resultado o entidad.

Si la tabla dinámica no se comporta como se esperaba, consulte [Troubleshooting the pivot](#) en la Guía del usuario de Amazon Detective.

Note

Si archiva un resultado de GuardDuty en la consola de Detective, ese resultado también se archiva en la consola GuardDuty.

Uso de la integración con un entorno multicuenta de GuardDuty

Si administra un entorno de varias cuentas en GuardDuty, debe agregar sus cuentas de miembro a Amazon Detective para ver las visualizaciones de los datos de Detective sobre los resultados y las entidades de esas cuentas.

Se recomienda utilizar la misma cuenta de administrador de GuardDuty para la cuenta de administrador de Detective. Para obtener más información sobre cómo añadir cuentas de miembros en Detective, consulte [Administración de cuentas](#) en la Guía del usuario de Amazon Detective.

Note

Detective es un servicio regional, lo que significa que debe habilitar Detective y agregar sus cuentas de miembros en cada región en la que quiera utilizar la integración.

Suspensión o deshabilitación de GuardDuty

Puede usar la consola de GuardDuty para suspender o deshabilitar el servicio GuardDuty. No se le cobra el uso de GuardDuty una vez suspendido el servicio.

- Todas las cuentas de miembros deben desasociarse o eliminarse para poder suspender o deshabilitar GuardDuty.
- Si suspende GuardDuty, dejará de supervisar la seguridad del entorno de AWS y de generar nuevos resultados. Los resultados existentes permanecerán intactos y no se verán afectados por la suspensión de GuardDuty. Puede elegir volver a habilitar GuardDuty más tarde.
- Al desactivar GuardDuty en una cuenta, se desactivará únicamente para la Región de AWS actualmente seleccionada. Si desea desactivar completamente GuardDuty, deberá desactivarlo en cada región en la que esté habilitado.
- Si deshabilita GuardDuty, los resultados y la configuración de GuardDuty existentes se perderán y no podrán recuperarse. Si desea guardar los resultados existentes, debe exportarlos antes de confirmar la desactivación de GuardDuty. Para obtener más información sobre cómo exportar resultados, consulte [Exportar los resultados generados a Amazon S3](#).
- Si ha habilitado la protección contra malware para S3 para uno o más buckets protegidos en la cuenta, la suspensión o desactivación de GuardDuty no afectará al estado de un bucket protegido en la protección contra malware para S3. Incluso después de suspender o desactivar GuardDuty, la cuenta no dejará de incurrir en los costos de uso asociados a la característica de protección contra malware para S3. Para obtener información sobre cómo desactivar la protección contra malware para S3, consulte [Desactivar la protección contra malware para S3 para un bucket protegido](#).

Suspensión o deshabilitación de GuardDuty

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Configuración.
3. En la sección Suspend GuardDuty, seleccione Suspend GuardDuty o Deshabilitar GuardDuty y, a continuación, confirme la acción.

Rehabilitación de GuardDuty después de la suspensión

1. Abra la consola de GuardDuty en <https://console.aws.amazon.com/guardduty/>.

2. En el panel de navegación, seleccione Configuración.
3. Elija Volver a habilitar GuardDuty.

Suscripción a los anuncios de Amazon SNS para GuardDuty

En esta sección se proporciona información sobre cómo suscribirse a Amazon SNS (Simple Notification Service) para anuncios de GuardDuty a fin de recibir notificaciones sobre nuevos tipos de resultados publicados, actualizaciones para los tipos de resultados existentes u otros cambios en funcionalidades. Las notificaciones están disponibles en todos los formatos que admite Amazon SNS.

El tema de SNS para GuardDuty envía anuncios sobre las actualizaciones del servicio GuardDuty en AWS a cualquier cuenta suscrita. Para recibir notificaciones sobre los resultados de su cuenta, consulte [Procesamiento de resultados de GuardDuty con Amazon EventBridge](#).

Note

Su usuario de IAM debe disponer de los permisos `sns::subscribe` para suscribirse a un tema de SNS.

Puede suscribir una cola de Amazon SQS a este tema de notificación, pero debe utilizar un ARN de tema que esté en la misma región. Para obtener más información, consulte [Tutorial: Subscribing an Amazon SQS queue to an Amazon SNS topic](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

También puede utilizar una función de AWS Lambda para desencadenar eventos cuando se reciban notificaciones. Para obtener más información, consulte [Invocación de funciones de Lambda mediante notificaciones de Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

Los ARN de tema de Amazon SNS para cada región se muestran a continuación.

Región de AWS	ARN del tema de Amazon SNS
Este de EE. UU. (Norte de Virginia) - us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements

Región de AWS	ARN del tema de Amazon SNS
Este de EE. UU. (Ohio) - us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
Oeste de EE. UU. (Norte de California) - us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
Oeste de EE. UU. (Oregón) - us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
Canadá (centro) - ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
Oeste de Canadá (Calgary) - ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
Europa (Estocolmo) - eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
Europa (Irlanda) - eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

Región de AWS	ARN del tema de Amazon SNS
Europa (Londres) - eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
Europa (París) - eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
Europa (Fráncfort) - eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
Europa (Zúrich): - eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
Asia-Pacífico (Hong Kong) - ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
Asia-Pacífico (Tokio) - ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
Asia-Pacífico (Seúl) - ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

Región de AWS	ARN del tema de Amazon SNS
Asia-Pacífico (Singapur) - ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
Asia-Pacífico (Sídney) - ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
Asia-Pacífico (Mumbai) - ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
América del Sur (São Paulo):) - sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
AWS GovCloud (Oeste de EE. UU) - us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
China (Pekín) - cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
China (Ningxia) - cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

Región de AWS	ARN del tema de Amazon SNS
Medio Oriente (Baréin):) - 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 (Milán) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Europa (España):) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (Este de EE. UU) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asia-Pacífico (Osaka): ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Asia-Pacífico (Yakarta):) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

Región de AWS	ARN del tema de Amazon SNS
Asia-Pacífico (Hyderabad):) - ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
Asia-Pacífico (Melbourne):) - ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
Asia-Pacífico (Malasia) - ap-southeast-5	arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements
Israel (Tel Aviv) - il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements
Asia-Pacífico (Tailandia):) - ap-southeast-7	arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements
México (centro):) - mx-central-1	arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements
Asia-Pacífico (Taipéi) - ap-east-2	arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements

Suscripción al correo electrónico de notificación de actualizaciones de GuardDuty en la Consola de administración de AWS

1. Abra la consola de Amazon SNS en <https://console.aws.amazon.com/sns/v3/home>.
2. En la lista de regiones, elija la misma región que la del ARN del tema al que desea suscribirse. En este ejemplo se utiliza la región `us-west-2`.
3. En el panel de navegación izquierdo, elija Subscriptions (Suscripciones), Create subscription (Crear suscripción).
4. En el cuadro de diálogo Create Subscription (Crear suscripción), en Topic ARN (ARN del tema), pegue el ARN del tema: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. En Protocolo, elige Correo electrónico. En Endpoint (Punto de enlace), escriba una dirección de correo electrónico que pueda utilizar para recibir la notificación.
6. Elija Crear suscripción.
7. En su aplicación de correo electrónico, abra el mensaje de Notificaciones de AWS y abra el enlace para confirmar la suscripción.

El navegador web muestra una respuesta de confirmación de Amazon SNS.

Suscripción al correo electrónico de notificación de actualizaciones de GuardDuty con la AWS CLI

1. Ejecute el siguiente comando 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. En su aplicación de correo electrónico, abra el mensaje de Notificaciones de AWS y abra el enlace para confirmar la suscripción.

El navegador web muestra una respuesta de confirmación de Amazon SNS.

Formato de los mensajes de Amazon SNS

Un ejemplo de mensaje de notificación general de GuardDuty:

```
{
```

```

    "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+6p8Gy0vKCQaeBG7HZhR1AbpyVka7JSNR0/6ssyrljlg==",
    "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"
  }

```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```

{
  "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"
      ]
    }
  ]
}

```

A continuación se muestra un mensaje de ejemplo de notificación de actualizaciones de GuardDuty sobre nuevos resultados:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FINDINGS\", \"findingDetails\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html\", \"findingType\":\"UnauthorizedAccess:EC2/TorClient\", \"findingDescription\":\"This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as initial gateways into a Tor network. This traffic can indicate that this EC2 instance is acting as a client on a Tor network. A common use for a Tor client is to circumvent network monitoring and filter for access to unauthorized or illicit content. Tor clients can also generate nefarious Internet traffic, including attacking SSH servers. This activity can indicate that your EC2 instance is compromised.\"}]}\",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
  "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."
```

```
  ]]
}
```

A continuación se muestra un mensaje de ejemplo de notificación de actualizaciones de GuardDuty sobre actualizaciones de funcionalidades de GuardDuty:

```
{
  "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"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
  "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"
  ]]
}

```

A continuación se muestra un mensaje de ejemplo de notificación de actualizaciones de GuardDuty sobre resultados actualizados:

```

{
  "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"
}

```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```

{
  "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."
  }]
}

```

```
}
```

Cuotas de Amazon GuardDuty

Su Cuenta de AWS tiene cuotas predeterminadas —anteriormente conocidas como “límites”— para cada servicio de Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar aumentos para algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de GuardDuty, abra la [consola de Service Quotas](#). En el panel de navegación, elija Servicios de AWS y seleccione Amazon GuardDuty.

Para solicitar un aumento de cuota, consulte [Solicitud de un aumento de cuota](#) en la Guía de usuario de Service Quotas.

La Cuenta de AWS tiene las siguientes cuotas para Amazon GuardDuty por región.

Note

- Para conocer las cuotas específicas de la protección contra malware de GuardDuty para EC2, consulte [Cuotas en la protección contra malware de EC2](#).
- Para conocer las cuotas específicas de la protección contra malware para S3, consulte [Cuotas en la protección contra malware para S3](#).

Cuotas de GuardDuty por región

Recurso	Valor predeterminado	Comentarios
Detectores	1	El número máximo de recursos del detector que puede crear por cuenta de AWS por región. No puede solicitar un aumento de cuota.
Filtros	100	El número máximo de filtros guardados por cuenta de AWS por región.

Recurso	Valor predeterminado	Comentarios
		No puede solicitar un aumento de cuota.
Periodo de conservación de hallazgos	90 días	El número máximo de días que se guarda un hallazgo. No puede solicitar un aumento de cuota.
Direcciones IP y rangos de CIDR por lista de direcciones IP de confianza	2,000	Número máximo de direcciones IP y rangos de CIDR que se pueden incluir en una misma lista de direcciones IP de confianza. No puede solicitar un aumento de cuota.
Direcciones IP y rangos de CIDR por lista de direcciones IP de amenazas	250.000	Número máximo de direcciones IP y rangos de CIDR que se pueden incluir en una lista de direcciones IP de amenazas. No puede solicitar un aumento de cuota.

Recurso	Valor predeterminado	Comentarios
Lista de entidades por amenaza	1 000	El número máximo de entidades que puede incluir en una sola lista de entidades de amenaza. No puede solicitar un aumento de cuota.
Entidades por lista de entidades de confianza	1 000	El número máximo de entidades que puede incluir en una lista de entidades de confianza. No puede solicitar un aumento de cuota.
Tamaño máximo de archivo	35 MB	El tamaño máximo del archivo utilizado para cargar una lista de entidades o una lista de direcciones IP. No puede solicitar un aumento de cuota.
Cuentas de los miembros (por invitación)	5000	El número máximo de cuentas de miembro asociadas a una cuenta de administrador. No puede solicitar un aumento de cuota.

Recurso	Valor predeterminado	Comentarios
Cuentas de miembros	50 000	El número máximo de cuentas de miembro asociadas a una cuenta de administrador a través de AWS Organizations. Esto incluye las cuentas de miembro que se agregan a la organización mediante invitación. Este valor predeterminado depende de la cuota actual para las cuentas de miembro en AWS Organizations. La cantidad de cuentas de miembro de GuardDuty que se agreguen a través de AWS Organizations no puede superar la cantidad de cuentas de miembro de la organización. Para obtener información sobre la cantidad de Cuentas de AWS de una organización, consulte Valores máximos y mínimos en la Guía del usuario

Recurso	Valor predeterminado	Comentarios
		de AWS Organizations.
Conjuntos de información sobre amenazas (lista de direcciones IP)	6	Número máximo de listas de direcciones IP de amenazas que puede añadir por Cuenta de AWS y por región. No puede solicitar un aumento de cuota.
Conjuntos de IP de confianza (lista de direcciones IP)	1	La cantidad máxima de listas de direcciones IP de confianza que se pueden cargar y activar por Cuenta de AWS y por región. No puede solicitar un aumento de cuota.
Listas de entidades de amenazas	6	Número máximo de listas de entidades de amenazas que se pueden añadir por Cuenta de AWS y por región. No puede solicitar un aumento de cuota.

Recurso	Valor predeterminado	Comentarios
Lista de entidades de confianza	1	La cantidad máxima de listas de entidades de confianza que se pueden cargar y activar por Cuenta de AWS y por región. No puede solicitar un aumento de cuota.

Solución de problemas de Amazon GuardDuty

Si tiene problemas relacionados con una acción específica de GuardDuty, consulte los temas de esta sección.

Temas

- [Exportar resultados a Amazon S3: error de acceso](#)
- [Problemas de la protección contra malware para EC2](#)
- [Problemas de supervisión en tiempo de ejecución](#)
- [Otras cuestiones de solución de problemas](#)

Exportar resultados a Amazon S3: error de acceso

Al exportar resultados de GuardDuty a un bucket de Amazon S3 como destino de publicación, se puede generar un error de acceso si GuardDuty no logra acceder a dicho destino.

Después de configurar la exportación de resultados, si GuardDuty no logra exportarlos, se mostrará un mensaje de error en la página Configuración en la Consola de GuardDuty. Esto podría ocurrir si GuardDuty pierde acceso al recurso de destino. Por ejemplo, si el bucket de Amazon S3 se ha eliminado o se ha modificado el permiso de acceso al bucket. Esto también podría ocurrir si GuardDuty pierde acceso a la clave de AWS KMS utilizada para cifrar los datos en el bucket de Amazon S3. Cuando GuardDuty no logra exportar, envía una notificación al correo electrónico asociado a la cuenta para informar sobre el problema.

¿Cómo se resuelve el error de acceso?

Para solucionar el problema, verifique que los recursos correspondientes existan y que GuardDuty disponga de los permisos necesarios para acceder a estos.

Para obtener más información, consulte [Exportar los resultados generados a Amazon S3](#).

¿Qué ocurre si no se resuelve este error?

Si no soluciona el problema antes de que finalice el período de retención de resultados de 90 días en GuardDuty, estos no se exportarán. GuardDuty desactivará la configuración de exportación de resultados para esta cuenta en la región específica.

Para volver a exportar resultados, actualice los parámetros de configuración de la región en cuestión.

Problemas de la protección contra malware para EC2

En esta sección se describen los errores que podría experimentar al configurar o utilizar la protección contra malware para EC2.

Falta el permiso de administración AWS Organizations necesario al habilitar el análisis de malware iniciado por GuardDuty

Si desea administrar varias cuentas mediante AWS Organizations y recibe este error: `The request failed because you do not have required AWS Organization master permission.`; significa que le falta el permiso para habilitar el análisis de malware iniciado por GuardDuty para varias cuentas de su organización.

Para obtener información sobre la concesión de permisos a la cuenta de administración, consulte [Establecimiento de un acceso confiable para permitir el análisis de malware iniciado por GuardDuty](#).

Estoy iniciando un análisis de malware bajo demanda, pero se produce un error de falta de permisos necesarios.

Si recibe un error que indica que no tiene los permisos necesarios para iniciar un análisis de malware bajo demanda en una instancia de Amazon EC2, compruebe que ha adjuntado la política [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#) a su rol de IAM.

Si es miembro de una organización de AWS y sigue recibiendo el mismo error, conéctese con su cuenta de administración. Para obtener más información, consulte [SCP de AWS Organizations: acceso denegado](#).

Recibo un error **iam:GetRole** al trabajar con la protección contra malware para EC2.

Si recibe el error `Unable to get role:`

`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, significa que le falta el permiso para habilitar el análisis de malware iniciado por GuardDuty o utilizar el análisis de malware bajo demanda. Compruebe que ha adjuntado la política [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#) a su rol de IAM.

Soy una cuenta de administrador de GuardDuty que necesita habilitar el análisis de malware iniciado por GuardDuty pero no utiliza la política administrada de AWS: AmazonGuardDutyFullAccess para administrar GuardDuty.

- Configure el rol de IAM que utiliza con GuardDuty para disponer de los permisos necesarios para habilitar el análisis de malware iniciado por GuardDuty. Para obtener más información sobre los permisos necesarios, consulte [Crear un rol vinculado al servicio para la protección contra malware para EC2](#).
- Adjunte [Política administrada de AWS: AmazonGuardDutyFullAccess_v2 \(recomendada\)](#) al rol de IAM. Esto lo ayudará a habilitar el análisis de malware iniciado por GuardDuty para las cuentas de miembros.

Problemas de supervisión en tiempo de ejecución

En esta sección se describen los errores que se pueden producir al configurar o utilizar la Supervisión en tiempo de ejecución.

Problemas de cobertura en tiempo de ejecución

Cuando la cobertura en tiempo de ejecución de los recursos protegidos se encuentra en mal estado, la Consola de GuardDuty indica el tipo exacto de problema. Una vez que conozca el tipo de problema, utilice los siguientes documentos para conocer los pasos de solución de problemas correspondientes a cada tipo de recurso admitido:

- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon ECS-Fargate](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS](#)

Solución de problemas de error de memoria insuficiente en la Supervisión en tiempo de ejecución (solo compatible con Amazon EC2)

En esta sección se describen los pasos a seguir cuando se experimenta un error de falta de memoria basado en [Límite de CPU y memoria](#) para la implementación manual del agente de seguridad de GuardDuty.

Si `systemd` termina el agente de GuardDuty debido al problema de out-of-memory y se determina que asignar más memoria al agente es una solución razonable, podrá ajustar el límite de memoria.

1. Con el permiso de raíz, abra `/lib/systemd/system/amazon-guardduty-agent.service`.
2. Busque `MemoryLimit` y `MemoryMax`, y actualice ambos valores.

```
MemoryLimit=256M
MemoryMax=256M
```

3. Después de actualizar los valores, reinicie el agente de GuardDuty con el siguiente comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Ejecute el siguiente comando para ver el estado:

```
sudo systemctl status amazon-guardduty-agent
```

La salida esperada mostrará el nuevo límite de memoria:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Se producen errores inesperados en mi flujo de trabajo de AWS Step Functions

Si el contenedor de GuardDuty contribuyó al error en el flujo de trabajo, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon ECS-Fargate](#). Si el problema persiste, para evitar que se produzca un error en el flujo de trabajo ocasionado por el contenedor de GuardDuty, siga uno de los siguientes pasos:

- Agregue la etiqueta `GuardDutyManaged:false` al clúster de Amazon ECS asociado.
- Desactive la configuración automatizada del agente para AWS Fargate (solo ECS) a nivel de cuenta. Agregue la etiqueta de inclusión `GuardDutyManaged:true` al clúster de Amazon ECS asociado cuya supervisión desea continuar con el agente automatizado de GuardDuty.

Otras cuestiones de solución de problemas

Si no encuentra un escenario adecuado para su problema, consulte las siguientes opciones de solución de problemas:

- Para obtener información sobre problemas generales de IAM al acceder a <https://console.aws.amazon.com/guardduty/>, consulte [Solución de problemas de identidad y acceso de Amazon GuardDuty](#).
- Para obtener información sobre problemas de autenticación y autorización al acceder al AWS Console Home de AWS, consulte [Solución de problemas de IAM](#).

Regiones y puntos de conexión de Amazon GuardDuty

Para ver las Regiones de AWS donde está disponible Amazon GuardDuty, consulte los [Puntos de conexión de Amazon GuardDuty](#) en Referencia general de Amazon Web Services.

Se recomienda que habilite GuardDuty en todas las Regiones de AWS admitidas. Esto permite a GuardDuty generar resultados sobre la actividad no autorizada o inusual incluso en las regiones que no utiliza de forma activa. Esto también permite a GuardDuty supervisar los eventos de AWS CloudTrail en busca de las Regiones de AWS admitidas y reduce su capacidad para detectar actividades que involucren servicios globales.

Disponibilidad de características específicas por región

Una lista de diferencias regionales para especificar la disponibilidad de las características de GuardDuty.

API ListFindings y GetFindingsStatistics

Las API [GetFindingsStatistics](#) y [ListFindings](#) tienen una marca `consoleOnly` temporal. Cuando se utiliza una de estas API o ambas, la marca `consoleOnly` significa que la API puede obtener resultados hasta un límite máximo de 1000.

Malware Protection for EC2

GuardDuty admite la característica [Protección contra malware para EC2](#) en las [zonas locales dedicadas de AWS](#).

Protección de RDS

La protección de RDS no se admite en la región Asia Pacífico (Taipéi) (`ap-east-2`).

Compatibilidad general de la API

Las siguientes API de la referencia de API de Amazon GuardDuty pueden tener diferencias regionales debido a la falta de disponibilidad de algunos de los orígenes de datos o características en Regiones de AWS especificadas anteriormente:

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)

- [UpdateOrganizationConfiguration](#)
- [GetDetector](#)
- [GetMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

Tipos de resultados de Amazon EC2: [DefenseEvasion:EC2/UnusualDoHActivity](#) y [DefenseEvasion:EC2/UnusualDoTActivity](#)

En la siguiente tabla, se muestran las Regiones de AWS donde está disponible GuardDuty, pero estos dos tipos de resultados de Amazon EC2 aún no son compatibles.

Región de AWS	Código de región
Asia-Pacífico (Seúl)	ap-northeast-2
Asia-Pacífico (Osaka)	ap-northeast-3
Asia-Pacífico (Yakarta)	ap-southeast-3

AWS GovCloud (US)Regiones de

Para obtener información más actualizada, consulte [Amazon GuardDuty](#) en la Guía del usuario de AWS GovCloud (US).

Regiones de China

Para obtener información más actualizada, consulte [Feature availability and implementation differences](#).

Acciones y parámetros heredados de GuardDuty

Algunas de las acciones y los parámetros de la API han quedado obsoletos en Amazon GuardDuty, pero se siguen admitiendo. La práctica recomendada consiste en utilizar las acciones y los parámetros nuevos de la API que sustituyen a las opciones heredadas. En la tabla siguiente se comparan las acciones y los parámetros heredados y los nuevos.

Acciones y parámetros heredados	Acciones y parámetros nuevos	Comparación
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Con la misma implementación en ambas acciones, GuardDuty usa el término Administrator en DisassociateFromAdministratorAccount.
Parámetro autoEnable en DescribeOrganizationConfiguration y UpdateOrganizationConfiguration	autoEnableOrganizationMembers	Con autoEnableOrganizationMembers, la cuenta de administrador de GuardDuty puede auditar y aplicar GuardDuty para todas las cuentas de miembro con cualquiera de los valores. Con las API, la actualización de la configuración de todas las cuentas de miembros puede tardar hasta 24 horas en efectuarse. Para obtener más información sobre los posibles valores del campo autoEnableOrganizationMembers, consulte autoEnableOrganizationMembers .
Parámetro dataSources en las API	features	Desde marzo de 2023, puede configurar Protección contra malware de GuardDuty para EC2 y los nuevos planes de protección de GuardDuty

Acciones y parámetros heredados	Acciones y parámetros nuevos	Comparación
que figuran en Cambios en la API de GuardDuty en marzo de 2023 .		con features. Los planes de protección lanzados antes de marzo de 2023, incluida la protección contra malware para EC2, aún admiten la configuración mediante dataSources . Si utiliza las API para configurar un plan de protección, cada solicitud a la API puede incluir dataSources o features, pero no ambas opciones.

Historial de documentación de Amazon GuardDuty

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la última versión de la Guía del usuario de Amazon GuardDuty. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Funcionalidad actualizada: Runtime Monitoring	Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.9.0 del agente de seguridad para los recursos de Amazon ECS-AWS Fargate. Para obtener información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte las versiones de lanzamiento del agente de seguridad de GuardDuty .	28 de octubre de 2025
Funcionalidad actualizada: Runtime Monitoring	Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.9.0 del agente de seguridad para el recurso de Amazon EC2. Para obtener información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte las versiones de lanzamiento del agente de seguridad de GuardDuty .	23 de octubre de 2025

[Nuevo tipo de resultados de Runtime Monitoring: DefenseEvasion:Runtime/KernelModuleLoaded](#)

Runtime Monitoring de GuardDuty presenta un nuevo tipo de resultados que le ayuda a identificar las técnicas de evasión de la defensa en las que los actores de amenazas utilizan los módulos del kernel para eludir los controles de seguridad , modificar las operaciones del sistema y obtener acceso persistente al sistema. Para obtener más información, consulte [DefenseEvasion:Runtime/KernelModuleLoaded](#).

15 de octubre de 2025

[Funcionalidad actualizada: Runtime Monitoring](#)

Se agregó compatibilidad con la versión 1.34 de Kubernetes para las distribuciones del sistema operativo y la versión de agente de seguridad para el administrador de roles de GuardDuty SageMaker para los recursos de Amazon EKS. Para obtener más información, consulte [Validar los requisitos de arquitectura de Amazon EKS](#).

3 de octubre de 2025

Se agregó una guía de solución de problemas para las bases de datos de Amazon RDS???

Se agregó una guía para resolver los problemas de las bases de datos de RDS que pueden afectar a las capacidades de monitoreo de RDS Protection de GuardDuty, incluidos el estado de storage-full y los requisitos de réplica de lectura de RDS para PostgreSQL. Para obtener más información, consulte [Solución de problemas del monitoreo de RDS Protection](#).

15 de septiembre de 2025

[Funcionalidad actualizada: Runtime Monitoring](#)

Se agregó la distribución del sistema operativo Ubuntu Noble compatible con las versiones 6.13 y 6.14 del kernel para Runtime Monitoring de GuardDuty para Amazon EC2. Para obtener información sobre la versión del agente de EC2 compatible con esta distribución de sistema operativo, consulte [Validar los requisitos de arquitectura de Amazon EC2](#).

13 de septiembre de 2025

Funcionalidad actualizada:
RDS Protection

Se agregó compatibilidad con PostgreSQL 17 para RDS para bases de datos PostgreSQL monitoreadas por RDS Protection de GuardDuty. Para más información, consulte la [bases de datos compatibles](#) en Protección de RDS.

13 de septiembre de 2025

Funcionalidad actualizada:
protección contra malware para S3

La protección contra malware para S3 de GuardDuty aumenta la cuota predeterminada de archivos extraídos de 1000 a 10 000 archivos. Para obtener más información, consulte [Cuotas en la protección contra malware para S3](#).

3 de septiembre de 2025

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty lanza la nueva versión 1.11 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre la nueva versión del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

29 de agosto de 2025

Funcionalidad actualizada:
trabajar con listas

GuardDuty presenta listas personalizadas de entidades de amenazas y de confianza que admiten direcciones IP y nombres de dominio. GuardDuty sigue admitiendo la lista de direcciones IP y recomienda utilizar la lista de entidades para la detección de amenazas personalizada. Para obtener más información, consulte [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#).

15 de agosto de 2025

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty lanza una nueva versión 1.8.0 del agente de seguridad para los recursos de Amazon EC2 y Amazon ECS-AWS Fargate. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

12 de agosto de 2025

[Compatibilidad con la región Asia-Pacífico \(Taipéi\)](#)

Amazon GuardDuty ya está disponible en la región de Asia-Pacífico (Taipéi) (ap-east-2). Para activar GuardDuty en esta región, consulte [Primeros pasos](#). Puede recibir notificaciones sobre las actualizaciones de las funciones de GuardDuty y las detecciones de amenazas al [Suscribirse a los anuncios de GuardDuty de Amazon SNS en esta](#) región.

31 de julio de 2025

[Funcionalidad actualizada: protección contra malware para S3](#)

La protección contra malware para S3 ahora admite el análisis de objetos de hasta 100 GB, antes era de 5 GB. Esto incluye tanto los objetos individuales como los archivos extraídos. Para obtener más información, consulte [Cuotas de la protección contra malware para S3](#).

23 de julio de 2025

[Funcionalidad actualizada: se agregó el propietario esperado del bucket en las listas de amenazas e IP de confianza](#)

GuardDuty agregó el campo Propietario esperado del bucket para las listas de IP de confianza e IP de amenazas. En este campo opcional, puede especificar un ID de Cuenta de AWS que GuardDuty utilizará para verificar la propiedad del bucket de Amazon S3. Para obtener más información, consulte [Trabajo con listas de IP fiables y listas de amenazas](#).

16 de julio de 2025

[Funcionalidad actualizada:](#)
[Detección Extendida de Amenazas](#)

17 de junio de 2025

La Detección Extendida de Amenazas de GuardDuty ahora amplía la compatibilidad para los clústeres de Amazon EKS al correlacionar varias señales de seguridad entre los registros de auditoría de EKS, el comportamiento de los procesos en tiempo de ejecución y la actividad de la API de AWS. Active EKS Protection, Runtime Monitoring (con el complemento EKS) o ambas opciones para [maximizar la detección de amenazas](#). Para identificar posibles amenazas, GuardDuty presenta un nuevo tipo de resultado : [AttackSequence:EKS/CompromisedCluster](#). Para obtener más información, consulte [Detección Extendida de Amenazas](#).

Funcionalidad actualizada:
protección contra malware
para S3

La protección contra malware para S3 no admite el análisis de archivos con una relación de compresión extremadamente alta. Estos archivos se omitirán durante el análisis y se marcarán con un resultado de análisis de UNSUPPORTED. Para obtener más información, consulte [Estado potencial de análisis de objeto de S3 y estado del producto](#).

13 de junio de 2025

Funcionalidad actualizada:
Malware Protection for EC2

Malware Protection for EC2 ha añadido compatibilidad para escanear la mayoría de las instancias con productCode como marketplace. Esto se aplica al análisis de malware iniciado por GuardDuty y el análisis de malware bajo demanda. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

13 de junio de 2025

[Nueva política AmazonGuardDutyFullAccess_V2](#)

Se agregó una nueva política AmazonGuardDutyFullAccess_v2 con permisos para mejorar la seguridad al restringir las acciones administrativas a las entidades principales de servicio de GuardDuty. Para obtener información sobre esta política recomendada, consulte la [política administrada de AWS: AmazonGuardDutyFullAccess_v2](#)

4 de junio de 2025

[Compatibilidad regional ampliada para la protección de RDS](#)

4 de junio de 2025

La protección de RDS de GuardDuty está ya disponible en las regiones de México (centro), Asia-Pacífico (Tailandia) y Asia-Pacífico (Malasia). La protección de rDS ayuda a detectar comportamientos de inicio de sesión potencialmente sospechosos en Aurora MySQL, Aurora PostgreSQL (incluida la base de datos ilimitada) y RDS para PostgreSQL compatibles. En caso de detección de amenazas, GuardDuty genera un resultado de protección de RDS. Para obtener más información sobre las bases de datos compatibles y sobre cómo habilitar este plan de protección en las nuevas regiones compatibles, consulte [Protección de RDS](#).

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.7.1 del agente de seguridad para el recurso de Amazon EC2. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

3 de junio de 2025

Compatibilidad con la
Detección Extendida de
Amenazas

La Detección Extendida de Amenazas de GuardDuty ya está disponible en Asia-Pacífico (Tailandia) (ap-south-east-7). Sin necesidad de activación, detecta ataques en varias etapas que abarcan orígenes de datos, varios tipos de recursos de AWS y tiempo, dentro de una Cuenta de AWS. Cuando se detectan amenazas potenciales, se generan resultados de la secuencia de ataque. Para obtener más información, consulte [Detección Extendida de Amenazas](#).

12 de mayo de 2025

[Compatibilidad con la región de México \(centro\)](#)

Amazon GuardDuty está ahora disponible en la región de México (centro) (mx-central-1). Para activar GuardDuty en esta región, consulte [Primeros pasos](#). Puede recibir notificaciones sobre las actualizaciones de las funciones de GuardDuty y las detecciones de amenazas al [Suscribirse a los anuncios de GuardDuty de Amazon SNS en esta](#) región.

7 de mayo de 2025

[Funcionalidad actualizada: Runtime Monitoring](#)

Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.10.0 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

4 de abril de 2025

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.7.0 del agente de seguridad para los recursos de Amazon ECS-Fargate. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

4 de abril de 2025

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.7.0 del agente de seguridad para el recurso de Amazon EC2. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

3 de abril de 2025

Compatibilidad con la región Asia-Pacífico (Tailandia)

Amazon GuardDuty está ahora disponible en la región de Asia-Pacífico (Tailandia). Para obtener información sobre las características compatibles con esta región, consulte [Disponibilidad de características específicas de la región](#). Para activar GuardDuty en esta región, consulte [Primeros pasos](#). Puede recibir notificaciones sobre las actualizaciones de las características de GuardDuty y las detecciones de amenazas al [Suscribirse a los anuncios de GuardDuty de Amazon SNS](#).

1 de abril de 2025

Funcionalidad actualizada

El panel de resumen ahora muestra información basada en todos los resultados de seguridad generados, lo que elimina la limitación de 5000 resultados anteriores. Para obtener información sobre estas ideas, consulte el [panel de resumen de GuardDuty](#).

17 de marzo de 2025

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty ha publicado una nueva versión 1.9.0 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

2 de marzo de 2025

Funcionalidad actualizada:
Runtime Monitoring

Runtime Monitoring de GuardDuty ha agregado un nuevo tipo de problema de cobertura (agente no aprovisionado) para los recursos de Amazon EC2. Para obtener información sobre la solución de este problema, consulte [Solución de problemas de cobertura del tiempo de ejecución de Amazon EC2](#).

21 de febrero de 2025

[Funcionalidad actualizada:](#)
[Runtime Monitoring](#)

Runtime Monitoring de GuardDuty lanza nuevos agentes de seguridad para los recursos de Amazon EC2 y Amazon ECS-Fargate. Para obtener más información sobre las nuevas versiones del agente y una lista de los recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de seguridad de GuardDuty](#).

6 de febrero de 2025

[Compatibilidad con GuardDuty en la región de Asia-Pacífico \(Malasia\) existente](#)

La Detección Extendida de Amenazas de GuardDuty ya está disponible en la región de Asia-Pacífico (Malasia). Para obtener más información, consulte [Detección Extendida de Amenazas](#).

28 de enero de 2025

[Compatibilidad con la región Asia-Pacífico \(Malasia\)](#)

Amazon GuardDuty está disponible ahora en la región de Asia-Pacífico (Malasia). Para obtener información sobre las características compatibles con esta región, consulte [Disponibilidad de características específicas de la región](#). Para activar GuardDuty en esta región, consulte [Primeros pasos](#). Puede recibir notificaciones sobre las actualizaciones de las características de GuardDuty y las detecciones de amenazas al [Suscribirse a los anuncios de GuardDuty de Amazon SNS](#).

16 de enero de 2025

[Funcionalidad actualizada: Runtime Monitoring](#)

Runtime Monitoring de GrandDuty ha actualizado la información adicional y los pasos de solución de problemas relacionados con la cobertura de Amazon ECS-Fargate relacionados con el agente no aprovisionado. Para obtener más información sobre el tipo de problema del agente no aprovisionado, consulte [Solución de problemas de cobertura del tiempo de ejecución de Amazon ECS-Fargate](#).

8 de enero de 2025

Nuevo tipo de resultado:[Policy:IAMUser/ShortTermRootCredentialUsage](#)

GuardDuty presenta un nuevo tipo de resultado que le avisa cuando se utilizan credenciales de usuario restringidas, creadas para las Cuentas de AWS que figuran en su entorno, para realizar solicitudes a los Servicios de AWS. Para obtener más información, consulte [Policy:IAMUser/ShortTermRootCredentialUsage](#).

8 de enero de 2025

Nueva característica:[Detección Extendida de Amenazas de GuardDuty](#)

GuardDuty anuncia la Detección Extendida de Amenazas para detectar secuencias de ataques en varias etapas que abarcan los orígenes de datos fundamentales y los recursos de AWS de GuardDuty en su Cuenta de AWS durante un tiempo específico. Sin costo adicional, esta función se habilita automáticamente para todas las cuentas que tengan GuardDuty activado. Esta característica anuncia dos nuevos tipos de resultados de GuardDuty, denominados [tipos de resultados de secuencias de ataque](#). Para obtener más información, consulte [Detección Extendida de Amenazas](#).

1 de diciembre de 2024

[Funcionalidad de multiservicio mejorada: Runtime Monitoring y Malware Protection for EC2](#)

1 de diciembre de 2024

Impacto de las nuevas características de Amazon Elastic Kubernetes Service (Amazon EKS) en las características de Amazon GuardDuty:

- Modo automático de Amazon EKS: tanto Runtime Monitoring para Amazon EKS como Malware Protection for EC2 lo admiten.
- Nodos híbridos de Amazon EKS: tanto Runtime Monitoring para Amazon EKS como Malware Protection for EC2 los admiten.

Para obtener más información, consulte [Cómo funciona Runtime Monitoring con los clústeres de Amazon EKS y Malware Protection for EC2](#).

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EKS](#)

Runtime Monitoring ha lanzado una nueva versión de agente 1.8.1 (v1.8.1-eks-build.2) para los recursos de Amazon EKS. Con esta nueva versión del agente, GuardDuty amplía la compatibilidad con Runtime Monitoring para los recursos de Amazon EKS que se ejecutan en RedHat, CentOS y Fedora. Para obtener más información, consulte [Validar los requisitos de arquitectura](#). Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para recursos de Amazon EKS](#).

23 de noviembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EC2](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión 1.5.0 del agente para los recursos de Amazon EC2. Con esta nueva versión del agente, GuardDuty amplía la compatibilidad con Runtime Monitoring para los recursos de Amazon EC2 que se ejecutan en RedHat, CentOS y Fedora. Para obtener más información, consulte [Validar los requisitos de arquitectura](#). Para obtener información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para recursos de Amazon EC2](#).

20 de noviembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon ECS-Fargate](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.5.0 para los recursos de Amazon ECS-Fargate. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para AWS Fargate \(solo Amazon ECS\)](#).

14 de noviembre de 2024

[Funcionalidad actualizada en la protección contra malware para EC2](#)

GuardDuty Malware Protection for EC2 ha añadido tres tipos de detección de Runtime Monitoring a la lista de [resultados que invocan el análisis de malware iniciado por GuardDuty](#) en instancias de Amazon EC2. Las cuentas que hayan activado Malware Protection for EC2 observarán el análisis de malware iniciado por GuardDuty cuando este genere alguno de los siguientes resultados:

- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

7 de noviembre de 2024

Funcionalidad actualizada en RDS Protection

RDS Protection de GuardDuty añade la nueva versión 16.4-limitless del motor de la [base de datos ilimitada Aurora PostgreSQL](#) a la lista de bases de datos compatibles. Si las Cuentas de AWS ya tienen habilitada RDS Protection, GuardDuty empezará automáticamente a supervisar el comportamiento de inicio de sesión de la base de datos ilimitada. Las cuentas que ya hayan utilizado la versión de prueba gratuita de 30 días de RDS Protection incurrirán en los costos de uso asociados a la base de datos ilimitada, junto con otras bases de datos compatibles que estén monitoreadas. Para obtener más información, consulte [Protección de RDS](#).

6 de noviembre de 2024

[Expansión regional - GuardDuty e integración de AWS PrivateLink](#)

GuardDuty ahora amplía la compatibilidad con regiones para [Amazon GuardDuty y los puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#).

Anteriormente, la compatibilidad con regiones estaba disponible para el Este de EE. UU. (Norte de Virginia), Europa (Irlanda) e Israel (Tel Aviv). Esta compatibilidad ahora se extiende a todas las Regiones de AWS donde GuardDuty esté disponible. Para obtener más información sobre las diferencias regionales, consulte [Disponibilidad de características específicas por región](#).

6 de noviembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon ECS-Fargate](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.4.1 para los recursos de Amazon ECS-Fargate. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para AWS Fargate \(solo Amazon ECS\)](#).

24 de octubre de 2024

[Compatibilidad adicional con las operaciones de etiquetado de GuardDuty CloudFormation](#)

GuardDuty ahora permite actualizar la clave y el valor de las etiquetas, así como las etiquetas a nivel de pila. Para ello, agregue el permiso `guardduty:tagResource` al rol de IAM. Para obtener información sobre GuardDuty CloudFormation, consulte la [referencia del tipo de recurso de Amazon GuardDuty](#) en la Guía del usuario de AWS CloudFormation.

24 de octubre de 2024

[Funcionalidad actualizada en la protección contra malware para S3 de GuardDuty3](#)

Al habilitar la protección contra malware para S3, puede elegir un rol de servicio que tenga los permisos necesarios para realizar acciones de análisis de malware en su nombre. Para obtener más información sobre cómo habilitar la protección contra malware para S3, consulte [Configurar la protección contra malware para S3 para el bucket de S3](#).

22 de octubre de 2024

Funcionalidad actualizada

GuardDuty mejora el tipo de resultado [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#) para detectar el uso de credenciales de AWS de la instancia de Amazon EC2 desde puntos de conexión de VPC (AWS PrivateLink) en Cuentas de AWS que no están asociadas al rol de instancia de Amazon EC2. Esta nueva función de GuardDuty detecta un posible uso indebido de las credenciales de la instancia Amazon EC2 y proporciona un contexto de la Cuenta de AWS remota mediante la extracción de las credenciales de sesión. Para obtener más información sobre los puntos de conexión de servicio de AWS compatibles con esta nueva detección, consulte [Registrar los eventos de actividad de la red](#) en la Guía del usuario de AWS CloudTrail

21 de octubre de 2024

Funcionalidad actualizada:
Supervisión en tiempo de
ejecución de GuardDuty

La Supervisión en tiempo de ejecución de GuardDuty ha agregado los siguientes tres tipos de resultados que notifican cuando se ejecutan comandos sospechosos en una instancia de Amazon EC2 o en una carga de trabajo de contenedor dentro del entorno de AWS:

10 de octubre de 2024

- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

Nueva característica:
compatibilidad agregada con
puntos de conexión de VPC

GuardDuty ahora está integrado con AWS PrivateLink y admite puntos de conexión de VPC. Para obtener más información sobre la integración con AWS PrivateLink, consulte [Amazon GuardDuty y puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#).

17 de septiembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EKS](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.7.1 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para Amazon EKS](#).

13 de septiembre de 2024

[Funcionalidad actualizada en la protección contra malware para S3](#)

La protección contra malware para S3 ha agregado un nuevo campo, `s3Throttled`, al esquema del resultado del análisis de objetos de S3 en Amazon EventBridge (EventBridge). El campo `s3Throttled` indica si hubo o no un retraso en la carga o recuperación de almacenamiento de los buckets de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte [Supervisión de los análisis de objetos de S3 con Amazon EventBridge](#).

13 de septiembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EC2](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.3.1 para los recursos de Amazon EC2. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para Amazon EC2](#).

12 de septiembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon ECS-Fargate](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.3.1 para los recursos de Amazon ECS-Fargate. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para AWS Fargate \(solo Amazon ECS\)](#).

11 de septiembre de 2024

[Rol vinculado al servicio \(SLR\) de GuardDuty actualizado](#)

GuardDuty ha actualizado el rol vinculado al servicio de modo que incluya el permiso `ec2:DescribeVpcs` en las acciones de Amazon EC2. Para obtener más información, consulte [Permisos del rol vinculado al servicio para GuardDuty](#).

22 de agosto de 2024

[Importante adición de contenidos](#)

GuardDuty agregó importantes actualizaciones de contenido a la característica de protección contra malware para S3. 20 de agosto de 2024

- Se han agregado nuevos ejemplos de esquemas de notificación de muestra para configurar reglas de Amazon EventBridge que permitan recibir notificaciones sobre el estado de los recursos del plan de protección contra malware y los resultados del análisis de objetos en S3. Para obtener más información, consulte [Supervisión de los análisis de objetos de S3 con Amazon EventBridge](#).
- Se ha agregado información sobre la [Solución de problemas de errores de etiquetas posteriores al análisis de objetos de S3](#).

[Funcionalidad actualizada en la Supervisión de tiempo de ejecución de GuardDuty: Amazon EC2](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión 1.3.0 del agente para los recursos de Amazon EC2. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para Amazon EC2](#). 19 de agosto de 2024

[Funcionalidad actualizada en la Supervisión de tiempo de ejecución de GuardDuty: Amazon EKS](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.7.0 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para clústeres de Amazon EKS](#).

17 de agosto de 2024

[Importante adición de contenidos](#)

GuardDuty ha agregado nueva información sobre la metodología de detección de malware y los motores de análisis que utiliza para las características de protección contra malware para S3 y protección contra malware para EC2. Para obtener más información, consulte [Motor de análisis de detección de malware de GuardDuty](#).

15 de agosto de 2024

[Nueva característica: protección de las cargas de trabajo de IA](#)

La detección de amenazas fundamental de GuardDuty y la protección de Lambda ayudan a aumentar el nivel de seguridad y a detectar amenazas para las cargas de trabajo de IA basadas en AWS. Para obtener más información, consulte [Proteger las cargas de trabajo de IA con GuardDuty](#).

14 de agosto de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución de GuardDuty : Fargate \(solo Amazon ECS\)](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.3.0 para los recursos de AWS Fargate (solo Amazon ECS). Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para Fargate-ECS](#).

9 de agosto de 2024

[Funcionalidad actualizada: protección contra malware para S3](#)

Protección contra malware para S3 de GuardDuty aumenta la cuota de cantidad máxima de buckets de S3 de 10 a 25. Esta cuota se aplica a una Cuenta de AWS por cada Región de AWS. Para obtener más información, consulte [Protección contra malware para S3](#).

8 de agosto de 2024

[Actualizado: nuevos tipos de resultados en la Supervisión en tiempo de ejecución](#)

GuardDuty ha agregado dos nuevos tipos de resultados de la Supervisión en tiempo de ejecución que ayudan a detectar amenazas que implican la creación sospechosa de intérpretes de comandos en el recurso supervisado, así como la escalada de privilegios en la que un proceso eleva sospechosamente sus privilegios a raíz.

6 de agosto de 2024

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[Actualizado: se integra con AWS Security Hub CSPM](#)

AWS Security Hub CSPM proporciona una lista de controles de seguridad de GuardDuty para evaluar los recursos y comprobar si cumplen la normativa y las prácticas recomendadas del sector de la seguridad. Para obtener más información, consulte [Utilizar controles de GuardDuty en Security Hub](#).

11 de julio de 2024

[Script de herramienta de pruebas de GuardDuty actualizado para resultados](#)

GuardDuty ahora admite más de 100 resultados con diferentes recursos de AWS en una cuenta dedicada. Para obtener más información, consulte [Probar los resultados de GuardDuty en cuentas dedicadas](#).

28 de junio de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha publicado una nueva versión 1.2.0 del agente de seguridad para el recurso de Amazon EC2. Para obtener información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para instancias de Amazon EC2](#). Para obtener información sobre la actualización manual del agente de seguridad a esta versión, consulte [Administrar manualmente el agente de seguridad para una instancia de Amazon EC2](#).

13 de junio de 2024

[Nueva característica: protección contra malware para la disponibilidad regional de S](#)

La protección contra malware para S3 de GuardDuty ahora se encuentra disponible en todas las regiones comerciales donde GuardDuty está disponible. Esta funcionalidad ayuda a analizar los objetos recién cargados en los buckets de Amazon S3 en busca de malware potencial y cargas sospechosas, así como a tomar medidas para aislarlos antes de que se ingieran en los procesos posteriores. Para obtener información sobre cómo habilitar la protección contra malware para S3, consulte [Protección contra malware para S3 de GuardDuty](#).

12 de junio de 2024

Nueva característica: protección contra malware para S3

11 de junio de 2024

GuardDuty anuncia la disponibilidad general de la protección contra malware para S3, que ayuda a analizar los objetos recién cargados en los buckets de Amazon S3 en busca de malware potencial y cargas sospechosas, así como a tomar medidas para aislarlos antes de que se ingieran en los procesos posteriores. Esta característica está completamente administrada por AWS. GuardDuty publica el resultado del análisis del objeto de S3 en el bus de eventos predeterminado de EventBridge. Puede permitir que GuardDuty agregue etiquetas a los objetos de S3 analizados. Puede crear flujos de trabajo posteriores, como el aislamiento en un bucket de cuarentena, o definir políticas de bucket mediante etiquetas que impidan a los usuarios o aplicaciones acceder a determinados objetos. Para obtener más información, consulte [Protección contra malware para S3 de GuardDuty](#). Actualmente está disponible en las siguientes regiones:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- Europa (Irlanda)
- Europa (Fráncfort)
- Europa (Estocolmo)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Asia-Pacífico (Singapur)

[Política de AmazonGuardDutyFullAccess actualizada](#)

Permiso agregado que permite transmitir un rol de IAM a GuardDuty al habilitar la protección contra malware para S3. Para obtener más información sobre esta actualización de la política, consulte la [política administrada de AWS: AmazonGuardDutyFullAccess](#). 10 de junio de 2024

[Funcionalidad actualizada en la protección de RDS de GuardDuty](#)

La protección de RDS amplía la compatibilidad para supervisar la actividad de inicio de sesión en las bases de datos de RDS para PostgreSQL. Como parte de esta ampliación, GuardDuty comenzará a supervisar automáticamente los datos de inicio de sesión en bases de datos de RDS para PostgreSQL de las cuentas que ya hayan habilitado la protección de RDS de GuardDuty. Para obtener más información, consulte [Protección de RDS](#).

6 de junio de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución de GuardDuty : Fargate \(solo Amazon ECS\)](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.2.0 para los recursos de AWS Fargate (solo Amazon ECS). Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para Fargate-ECS](#).

31 de mayo de 2024

[Funcionalidad actualizada en Malware Protection for EC2 de GuardDuty2](#)

Para cada volumen de Amazon EBS asociado a las instancias de Amazon EC2 y las cargas de trabajo de contenedores, la protección contra malware de GuardDuty para EC2 ha incrementado el tamaño del volumen de EBS que analiza, para alcanzar hasta 2048 GB. Para obtener información sobre el análisis de los volúmenes de Amazon EBS asociados a las instancias, consulte [Malware Protection for EC2 de GuardDuty](#).

29 de mayo de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

Supervisión en tiempo de ejecución para los recursos de Amazon ECS-Fargate ahora permite detectar posibles amenazas en las tareas lanzadas por AWS Batch y AWS CodePipeline. Para obtener más información, consulte [Cómo funciona la Supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#).

28 de mayo de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.6.1 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [Historial de versiones del agente del complemento EKS](#).

14 de mayo de 2024

[Compatibilidad regional ampliada para la Supervisión en tiempo de ejecución](#)

GuardDuty amplía la compatibilidad con la Supervisión en tiempo de ejecución a la región de Oeste de Canadá (Calgary) (Calgary). Para obtener información sobre cómo comenzar a utilizar la Supervisión en tiempo de ejecución, consulte [Habilitar la Supervisión en tiempo de ejecución](#).

7 de mayo de 2024

[Compatibilidad regional ampliada para RDS Protection](#)

GuardDuty amplía la compatibilidad con RDS Protection a las siguientes Regiones de AWS:

3 de mayo de 2024

- Oeste de Canadá (Calgary)
- Asia-Pacífico (Hyderabad)
- Europa (España)
- Europa (Zúrich)
- Medio Oriente (EAU)
- Israel (Tel Aviv)
- Asia-Pacífico (Melbourne)

Para obtener información sobre cómo habilitar esta característica, consulte [Protección de RDS](#).

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.1.0 para los recursos de AWS Fargate (solo Amazon ECS). Para obtener más información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para Fargate-ECS](#).

1 de mayo de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.6.0 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [Historial de versiones del agente del complemento EKS](#).

29 de abril de 2024

[Compatibilidad con IPAddress v6](#)

GuardDuty ha agregado compatibilidad con IPAddress v6 tanto para detalles de IP locales como remotos. Puede utilizar los [atributos de filtro](#) asociados para filtrar los resultados de GuardDuty o [crear reglas de supresión](#).

18 de abril de 2024

[Experiencia de consola actualizada para configurar la exportación de resultados](#)

GuardDuty ha actualizado la experiencia de la consola para exportar los resultados generados en las Cuentas de AWS a un bucket de Amazon S3. Para obtener más información, consulte [Exportar resultados de GuardDuty](#).

1 de abril de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha publicado una nueva versión 1.1.0 del agente de seguridad para el recurso de Amazon EC2. Esta versión admite la configuración automatizada del agente de GuardDuty en la Supervisión en tiempo de ejecución para instancias de Amazon EC2. Para obtener información sobre las notas de la versión, consulte [Agente de seguridad de GuardDuty para instancias de Amazon EC2](#).

28 de marzo de 2024

[Disponibilidad general de la Supervisión en tiempo de ejecución para las instancias de Amazon EC](#)

28 de marzo de 2024

GuardDuty anuncia la disponibilidad general (GA) de la Supervisión en tiempo de ejecución para las instancias de Amazon EC2. Ahora, tiene la opción de [habilitar la configuración automatizada del agente](#) que permite a GuardDuty instalar y administrar el agente de seguridad para las instancias de Amazon EC2 en su nombre. Con el agente automatizado de GuardDuty, también puede utilizar etiquetas de inclusión o exclusión para informar a GuardDuty que instale y administre el agente de seguridad únicamente en instancias de Amazon EC2 seleccionadas. Para obtener más información, consulte [Cómo funciona el Monitoreo de tiempo de ejecución con las instancias de Amazon EC2](#).

Lista de nuevos tipos de resultados publicados con esta disponibilidad general

- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)

- [DefenseEvasion:Runtime/
PtraceAntiDebugging](#)
- [Execution:Runtime/
MaliciousFileExecuted](#)

[Amazon GuardDuty ha actualizado el rol vinculado al servicio \(SLR\)](#)

26 de marzo de 2024

Utilice acciones de AWS Systems Manager para administrar asociaciones de SSM en instancias de Amazon EC2 cuando habilite la Supervisión en tiempo de ejecución de GuardDuty con el agente automatizado para Amazon EC2. Cuando la configuración automatizada del agente de GuardDuty está desactivada, GuardDuty solo considera aquellas instancias de EC2 que tienen una etiqueta de inclusión (GuardDuty Managed :true).

- En la siguiente lista aparecen los nuevos permisos:

```
"ssm:DescribeAssociation",  
"ssm:DeleteAssociation",  
"ssm:UpdateAssociation",  
"ssm:CreateAssociation",  
"ssm:StartAssociationsOnce",  
"ssm:AddTagsToResource",  
"ssm:CreateAssociation",  
"ssm:UpdateAssociation",  
"ssm:SendCommand",
```

```
"ssm:GetCommandInvocation"
```

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

Con la más reciente versión del agente de seguridad de GuardDuty (complemento) v1.5.0 para Amazon EKS, la Supervisión en tiempo de ejecución ahora permite configurar parámetros específicos del agente de seguridad de GuardDuty, como la configuración de CPU y memoria, ajustes de `PriorityClass` y configuración de políticas de DNS. Para obtener más información, consulte [Configurar los parámetros del agente de seguridad de GuardDuty \(complemento de EKS\)](#).

7 de marzo de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.5.0 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [Historial de versiones del agente del complemento EKS](#).

7 de marzo de 2024

[Compatibilidad para Oeste de Canadá \(Calgary\)](#)

Amazon GuardDuty ahora se encuentra disponible en la región Oeste de Canadá (Calgary). Es posible que algunos de los planes de protección de GuardDuty no estén disponibles en esta región. Para obtener la información más reciente, consulte [Regiones y puntos de conexión](#).

6 de marzo de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

Las versiones 1.0.0 y 1.1.0 del agente de seguridad GuardDuty para clústeres de Amazon EKS dejarán de recibir soporte a partir del 14 de mayo de 2024. Para obtener información sobre los pasos que puede dar antes de que finalice el soporte estándar, consulte [Agente de seguridad de GuardDuty para clústeres de Amazon EKS](#).

16 de febrero de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución es compatible con la [versión más reciente de Kubernetes 1.29](#) con la versión 1.4.1 del agente de seguridad existente. La compatibilidad ha estado disponible desde el lanzamiento de esta versión de Kubernetes. Para obtener información sobre las versiones de Kubernetes compatibles, consulte [Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty](#).

16 de febrero de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: disponibilidad regional](#)

12 de febrero de 2024

La Supervisión en tiempo de ejecución de GuardDuty ahora admite Amazon VPC compartida dentro del mismo AWS Organizations. [El rol vinculado al servicio \(SLR\) de GuardDuty](#) tiene un nuevo permiso, `organizations:DescribeOrganization`, que ayuda a recuperar el ID de organización para la cuenta de Amazon VPC compartida para establecer la política de punto de conexión. Para obtener información sobre los requisitos previos para utilizar un punto de conexión de Amazon VPC compartida en la Supervisión en tiempo de ejecución, consulte [Compatibilidad con Amazon VPC compartida](#). Esta capacidad está disponible en todas las regiones en las que GuardDuty admite la Supervisión en tiempo de ejecución.

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: disponibilidad regional](#)

La Supervisión en tiempo de ejecución de GuardDuty ahora admite Amazon VPC compartida dentro del mismo AWS Organizations. [El rol vinculado al servicio \(SLR\) de GuardDuty](#) tiene un nuevo permiso, `organizations:DescribeOrganization`, que ayuda a recuperar el ID de organización para la cuenta de Amazon VPC compartida para establecer la política de punto de conexión. Para obtener información sobre los requisitos previos para utilizar un punto de conexión de Amazon VPC compartida en la Supervisión en tiempo de ejecución, consulte [Compatibilidad con Amazon VPC compartida](#). Actualmente, esta capacidad está disponible en algunas de las Regiones de AWS. Para obtener más información, consulte [Regiones y puntos de enlace](#).

9 de febrero de 2024

[Funcionalidad actualizada con compatibilidad con nuevas Regiones de AWS: Malware Protection for EC2](#)

Malware Protection for EC2 ahora admite el análisis de los volúmenes de EBS cifrados con Claves administradas por AWS en la región de Oeste de EE. UU. (Oregón).

6 de febrero de 2024

[Funcionalidad actualizada con compatibilidad con nuevas Regiones de AWS: Malware Protection for EC2](#)

5 de febrero de 2024

Malware Protection for EC2 ahora admite el análisis de los volúmenes de EBS cifrados con Claves administradas por AWS en las [siguientes Regiones de AWS](#):

- Asia-Pacífico (Singapur) (ap-southeast-1)
- Europa (Fráncfort) (eu-central-1)
- Asia-Pacífico (Osaka) (ap-northeast-3)
- Este de EE. UU. (Ohio) (us-east-2)
- Europa (Milán) (eu-south-1)
- Asia-Pacífico (Tokio) (ap-northeast-1)
- Asia-Pacífico (Seúl) (ap-northeast-2)
- Canadá (centro) (ca-central-1)
- Europa (Irlanda) (eu-west-1)
- Este de EE. UU. (Norte de Virginia) (us-east-1)

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución de GuardDuty ha publicado una nueva versión del agente de seguridad de GuardDuty (v1.0.2) para las instancias de Amazon EC2. Esta versión del agente incluye compatibilidad con las AMI de Amazon ECS más recientes. Para obtener más información sobre el historial de versiones del agente, consulte [Agente de seguridad GuardDuty para instancias de Amazon EC2](#).

2 de febrero de 2024

[Funcionalidad actualizada con compatibilidad con nuevas Regiones de AWS: Malware Protection for EC2](#)

Malware Protection for EC2 ahora admite el análisis de los volúmenes de Amazon EBS cifrados con Claves administradas por AWS en las [siguientes Regiones de AWS:](#)

31 de enero de 2024

- Europa (Londres) (eu-west-2)
- Europa (Estocolmo) (eu-north-1)
- Asia Pacífico (Hong Kong) (ap-east-1)
- África (Ciudad del Cabo) (af-south-1)
- Medio Oriente (Baréin) (me-south-1)
- Asia-Pacífico (Hyderabad) (ap-south-2)
- Europa (España) (eu-south-2)
- Asia-Pacífico (Melbourne) (ap-southeast-4)
- Asia-Pacífico (Sídney) (ap-southeast-2)
- Israel (Tel Aviv) (il-central-1)

[Administración de cuentas con actualizada AWS Organizations](#)

Se reorganizó el contenido bajo [Administrar cuentas con AWS Organizations](#), se agregaron pasos para cambiar la cuenta de administrador delegado de GuardDuty y se actualizó [Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro](#).

30 de enero de 2024

[Funcionalidad actualizada con compatibilidad para nuevas Regiones de AWS](#)

Malware Protection for EC2 ahora admite el análisis de los volúmenes de EBS cifrados con Claves administradas por AWS en las [siguientes Regiones de AWS](#):

29 de enero de 2024

- Asia-Pacífico (Yakarta) (ap-southeast-3)
- Oeste de EE. UU. (Norte de California) (us-west-1)
- Medio Oriente (EAU) (me-central-1)
- Europa (Zúrich) (eu-central-2)
- Asia-Pacífico (Bombay) (ap-south-1)
- América del Sur (São Paulo) (sa-east-1)

[Funcionalidad actualizada en Malware Protection for EC2](#)

Malware Protection for EC2 ahora admite el análisis de los volúmenes de EBS cifrados mediante Claves administradas por AWS.

[El rol vinculado al servicio \(SLR\) de Malware Protection for EC2](#) cuenta con

dos nuevos permisos:

GetSnapshotBlock y
ListSnapshotBlocks

. Estos permisos ayudarán a GuardDuty a obtener la instantánea de un volumen de EBS (cifrado con Clave administrada de AWS) de la Cuenta de AWS y copiarlo en la [cuenta de servicio de GuardDuty](#) antes de iniciar el análisis de malware.

Actualmente, esta funcionalidad solo se encuentra disponible en Europa (París) (eu-west-3). Para obtener más información, consulte [Volúmenes admitidos para el análisis de malware](#).

25 de enero de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución de GuardDuty ha lanzado una nueva versión del agente de seguridad de GuardDuty (v1.0.1) con ajustes generales de rendimiento y mejoras. Para obtener más información sobre el historial de versiones del agente, consulte [Agente de seguridad GuardDuty para instancias de Amazon EC2](#).

23 de enero de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.4.1 para los recursos de Amazon EKS. Para más información, consulte [EKS add-on agent release history](#).

16 de enero de 2024

[La Supervisión en tiempo de ejecución ha lanzado un nuevo agente v1.4.0 para los recursos de Amazon EKS](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.4.0 para los recursos de Amazon EKS. Para más información, consulte [EKS add-on agent release history](#).

21 de diciembre de 2023

[Se han agregado tipos de resultados basados en machine learning \(ML\) de S3 y AWS CloudTrail a Europa \(Zúrich\), Europa \(España\), Asia-Pacífico \(Hyderabad\), Asia-Pacífico \(Melbourne\) e Israel \(Tel Aviv\)](#)

Los siguientes resultados de S3 y CloudTrail que identifican el comportamiento anómalo por medio del modelo de machine learning (ML) de detección de anomalías de GuardDuty ya se encuentran disponibles en las regiones de Europa (Zúrich) , Europa (España), Asia-Pacífico (Hyderabad), Asia Pacífico (Melbourne), e Israel (Tel Aviv):

21 de diciembre de 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 admite
50 000 cuentas de miembros a
través de AWS Organizations](#)

Un administrador delegado de GuardDuty ahora puede administrar un máximo de 50 000 cuentas de miembros a través de AWS Organizations. Esto también incluye un máximo de 5000 cuentas de miembro que se asocian a la cuenta de administrador de GuardDuty por invitación.

20 de diciembre de 2023

[La compatibilidad con la Supervisión en tiempo de ejecución de GuardDuty se amplía a 19 Regiones de AWS](#)

La Supervisión en tiempo de ejecución ya se encuentra disponible en Asia-Pacífico (Yakarta), Europa (París), Asia-Pacífico (Osaka), Asia-Pacífico (Seúl), Medio Oriente (Baréin), Europa (España), Asia-Pacífico (Hyderabad), Asia-Pacífico (Melbourne), Israel (Tel Aviv), Oeste de EE. UU. (Norte de California), Europa (Londres), Asia-Pacífico (Hong Kong), Europa (Milán), Medio Oriente (EAU), América del Sur (São Paulo), Asia-Pacífico (Bombay), Canadá (Centro), África (Ciudad del Cabo), Europa (Zúrich).

6 de diciembre de 2023

[GuardDuty amplía la capacidad de Supervisión en tiempo de ejecución](#)

Además de detectar amenazas a los clústeres de Amazon EKS, GuardDuty anuncia la disponibilidad general de la Supervisión en tiempo de ejecución para detectar amenazas a las cargas de trabajo de Amazon ECS y una versión preliminar para detectar amenazas a las instancias de Amazon EC2. Para obtener más información sobre qué Regiones de AWS admiten actualmente la Supervisión en tiempo de ejecución, consulte [Regiones y puntos de conexión](#).

26 de noviembre de 2023

[Amazon GuardDuty ha actualizado el rol vinculado al servicio \(SLR\)](#)

26 de noviembre de 2023

GuardDuty ha agregado nuevos permisos para utilizar las acciones de Amazon ECS para administrar y recuperar información sobre los clústeres de Amazon ECS, y administrar la configuración de la cuenta de Amazon ECS con `guarddutyActivate`. Las acciones que pertenecen a Amazon ECS también recuperan la información sobre las etiquetas asociadas a GuardDuty.

- Los siguientes permisos se han agregado como parte de la ampliación de la capacidad de [Supervisión en tiempo de ejecución de GuardDuty](#):

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

[Se han actualizado las políticas administradas de AWS](#)

16 de noviembre de 2023

GuardDuty agregó un nuevo permiso, `organizations:ListAccounts` a la política administrada de [AWS: AmazonGuardDutyFullAccess](#) y [AmazonGuardDutyReadOnlyAccess](#).

[GuardDuty lanzó nuevos tipos de resultados que utilizan la Supervisión de registros de auditoría de EKS.](#)

La Supervisión de registros de auditoría de EKS ahora admite los siguientes tipos de resultados en Asia-Pacífico (Melbourne) (ap-southeast-4).

11 de noviembre de 2023

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty lanzó nuevos tipos de resultados que utilizan la Supervisión de registros de auditoría de EKS.](#)

10 de noviembre de 2023

La Supervisión de registros de auditoría de EKS ahora admite los siguientes tipos de resultados en las regiones de Asia Pacífico (Hyderabad) (ap-south-2), Europa (Zúrich) (eu-central-2) y Europa (España) (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 lanzó nuevos tipos de resultados que utilizan la Supervisión de registros de auditoría de EKS.](#)

8 de noviembre de 2023

La Supervisión de registros de auditoría de EKS ahora admite los siguientes tipos de resultados. Estos tipos de resultados aún no están disponibles en las regiones Asia-Pacífico (Hyderabad) (ap-south-2), Europa (Zúrich) (eu-central-2), Europa (España) (eu-south-2) y Asia-Pacífico (Melbourne) (ap-southeast-4).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[La supervisión en tiempo de ejecución de EKS ha lanzado el nuevo agente v1.3.1](#)

La Supervisión en tiempo de ejecución de EKS ha lanzado una nueva versión 1.3.1 del agente que incluye importantes revisiones y actualizaciones de seguridad.

23 de octubre de 2023

[Nuevo atributo de filtro para resultados](#)

GuardDuty ha agregado un nuevo criterio para filtrar los resultados generados. El sufijo del dominio de solicitud de DNS proporciona el dominio de segundo y primer nivel implicado en la actividad que llevó a GuardDuty a generar el resultado.

17 de octubre de 2023

[La supervisión en tiempo de ejecución de EKS ha lanzado un nuevo agente de la versión 1.3.0 compatible con la versión 1.28 de Kubernetes 1.28](#)

La Supervisión en tiempo de ejecución de EKS lanzó una nueva versión de agente 1.3.0 que admite la versión 1.28 de Kubernetes. Se ha agregado compatibilidad con Ubuntu. Para más información, consulte [EKS add-on agent release history](#).

5 de octubre de 2023

[Se han agregado los tipos de resultados basados en S3 y el machine learning \(ML\) de AWS CloudTrail en las regiones Asia-Pacífico \(Yakarta\) y Medio Oriente \(EAU\)](#)

Los siguientes resultados de S3 y CloudTrail, que identifican el comportamiento anómalo mediante el modelo de machine learning (ML) de detección de anomalías (ML) de GuardDuty, ya están disponibles en las regiones de Asia Pacífico (Yakarta) y Medio Oriente (EAU):

20 de septiembre de 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](#)

[La supervisión en tiempo de ejecución de EKS en GuardDuty presenta la administración del agente de seguridad de GuardDuty a nivel de clúster](#)

La supervisión en tiempo de ejecución de EKS agrega compatibilidad para administrar el agente de seguridad de GuardDuty para clústeres de EKS individuales a fin de supervisar los eventos de tiempo de ejecución únicamente desde estos clústeres selectivos. La supervisión en tiempo de ejecución de EKS amplía esta capacidad con la compatibilidad con etiquetas.

13 de septiembre de 2023

[Malware Protection for EC2 de GuardDuty amplía la compatibilidad a más Regiones de AWS](#)

Malware Protection for EC2 ya está disponible en las regiones Asia-Pacífico (Hyderabad), Asia-Pacífico (Melbourne), Europa (Zúrich) y Europa (España).

11 de septiembre de 2023

[GuardDuty ya está disponible en la región Israel \(Tel Aviv\)](#)

24 de agosto de 2023

Se ha agregado la región Israel (Tel Aviv) a la lista de Regiones de AWS en las que GuardDuty está disponible ahora. Los siguientes planes de protección ya están disponibles en la región Israel (Tel Aviv):

- [EKS Protection](#) incluye la supervisión de registros de auditoría de EKS y la supervisión en tiempo de ejecución de EKS.
- [Protección de Lambda](#).
- [Protección contra malware para EC2](#).
- [Protección de S3](#).

Para obtener más información sobre la disponibilidad de planes de protección en la región Israel (Tel Aviv), consulte [Regiones y puntos de conexión](#).

[GuardDuty ha agregado una configuración de habilitación automática para su organización a nivel de plan de protección](#)

Actualice la configuración organizativa de los planes de protección de su región. Las posibles opciones de configuración son activar para todas las cuentas, habilitar automáticamente para las cuentas nuevas o no habilitar automáticamente para ninguna cuenta de su organización.

16 de agosto de 2023

[Los tipos de resultados de S3 que identifican comportamientos anómalos mediante el modelo de machine learning \(ML\) con detección de anomalías de GuardDuty ya están disponibles en la región Asia-Pacífico \(Osaka\)](#)

Los siguientes tipos de resultados ya están disponibles en la región Asia-Pacífico (Osaka):

10 de agosto de 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[La supervisión en tiempo de ejecución de EKS ya está disponible en la región Asia-Pacífico \(Melbourne\)](#)

La supervisión en tiempo de ejecución de EKS en la protección de EKS de GuardDuty ofrece la detección de amenazas en tiempo de ejecución para los clústeres de Amazon EKS en el entorno de AWS. Ya es compatible con la región Asia-Pacífico (Melbourne).

8 de agosto de 2023

[Se ha actualizado la lista de los resultados de GuardDuty que invocan un análisis de malware iniciado por este servicio](#)

Algunos tipos de resultados de la Supervisión en tiempo de ejecución de EKS ahora pueden invocar un análisis de malware iniciado por GuardDuty en su Cuenta de AWS.

19 de julio de 2023

[GuardDuty admite 10 000 cuentas de miembros a través de AWS Organizations](#)

Una cuenta de administrador de GuardDuty ahora puede administrar un máximo de 10 000 cuentas de miembro a través de AWS Organizations. Esto también incluye un máximo de 5000 cuentas de miembro que se asocian a la cuenta de administrador de GuardDuty por invitación.

29 de junio de 2023

[La supervisión en tiempo de ejecución de EKS anuncia tres nuevos tipos de resultados.](#)

La supervisión en tiempo de ejecución de EKS admite tres nuevos tipos de resultados que se basan en la técnica de inyección de procesos. Los nuevos tipos de resultados son DefenseEvasion:Runtime/ProcessInjection.Proc, DefenseEvasion:Runtime/ProcessInjection.Ptrace y DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.

22 de junio de 2023

[La supervisión en tiempo de ejecución de EKS ha lanzado un nuevo agente de la versión 1.2.0 compatible con la versión 1.27 de Kubernetes 1.27](#)

La Supervisión en tiempo de ejecución de EKS lanzó una nueva versión de agente 1.2.0 que también admite instancias basadas en ARM64. Se ha agregado compatibilidad con Bottlerocket. Para más información, consulte [EKS add-on agent release history](#).

16 de junio de 2023

[La consola de GuardDuty ofrece una vista resumida de sus resultados.](#)

El panel de resumen de la consola de GuardDuty proporciona una vista agregada de los resultados de GuardDuty. Actualmente, el panel muestra datos a través de varios widgets para los últimos 10 000 resultados generados para la cuenta (o cuentas de miembro si es una cuenta de administrador de GuardDuty) para la región actual.

12 de junio de 2023

[La supervisión de registros de auditoría de EKS ya está disponible en las regiones Asia-Pacífico \(Hyderabad\), Asia-Pacífico \(Melbourne\), Europa \(Zúrich\) y Europa \(España\)](#)

Habilite la supervisión de registros de auditoría de EKS (en la protección de EKS) para las cuentas para supervisar los registros de auditoría de EKS de los clústeres de Amazon EKS y analizarlos para detectar posibles actividades maliciosas o sospechosas.

1 de junio de 2023

[La supervisión de registros de auditoría de EKS ya está disponible en Medio Oriente \(EAU\)](#)

La Supervisión de registros de auditoría de EKS ya está disponible en Medio Oriente (EAU). Habilite la Supervisión de registros de auditoría de EKS para las cuentas para supervisar los registros de auditoría de EKS de los clústeres de Amazon EKS y analizarlos en busca de actividades potencialmente maliciosas y sospechosas.

3 de mayo de 2023

[Malware Protection for EC2 de GuardDuty anuncia el análisis de malware bajo demanda](#)

27 de abril de 2023

Malware Protection for EC2 ayuda a detectar la posible presencia de malware en los volúmenes de Amazon EBS asociados a las instancias y cargas de trabajo de contenedores de Amazon EC2. Ahora ofrece dos tipos de análisis: iniciados por GuardDuty y bajo demanda. El análisis de malware iniciado por GuardDuty inicia automáticamente un análisis sin agente en los volúmenes de Amazon EBS solo cuando GuardDuty genera uno de los [resultados que invoca el análisis de malware iniciado por GuardDuty](#). Para iniciar un análisis de malware bajo demanda para instancias de Amazon EC2 en su cuenta, puede proporcionar el nombre de recurso de Amazon (ARN) asociado a esa instancia de Amazon EC2. Para obtener más información sobre las diferencias entre ambos tipos de análisis, consulte [Malware Protection for EC2](#).

- [Análisis de malware iniciado por GuardDuty](#)
- [Análisis de malware bajo demanda](#)

[GuardDuty anuncia la protección de Lambda](#)

La protección de Lambda le ayuda a identificar posibles amenazas de seguridad en sus funciones de AWS Lambda.

20 de abril de 2023

- [Tipos de resultados de la protección de Lambda](#)
- [Corregir una función de Lambda potencialmente comprometida](#)

[GuardDuty ya está disponible en la región Asia-Pacífico \(Melbourne\)](#)

Se ha agregado la región Asia Pacífico (Melbourne) a la lista de Regiones de AWS en las que GuardDuty está disponible. Para obtener información sobre las características disponibles en esta región, consulte [Regiones y puntos de conexión](#).

19 de abril de 2023

[GuardDuty ha agregado 3 nuevos tipos de resultados de EC](#)

GuardDuty presenta nuevos tipos de resultados para detectar el uso de solucionadores de DNS externos y tecnologías de DNS cifrado. Para obtener información sobre las Regiones de AWS donde se admiten estos tipos de resultados, consulte [Regiones y puntos de conexión](#).

5 de abril de 2023

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

[GuardDuty anuncia la Supervisión en tiempo de ejecución de EKS en la Protección de EKS](#)

30 de marzo de 2023

La supervisión en tiempo de ejecución de EKS en la protección de EKS ofrece la detección de amenazas en tiempo de ejecución para los clústeres de Amazon EKS en el entorno de AWS. Utiliza un agente complementario (aws-guardduty-agent) de Amazon EKS que recopila los [eventos de tiempo de ejecución](#) de sus cargas de trabajo de EKS. Una vez que GuardDuty recibe estos eventos de tiempo de ejecución, los supervisa y analiza para identificar posibles amenazas de seguridad sospechosas. Para más información, consulte [Detalles de los resultados](#) y [Tipos de resultados de la Supervisión en tiempo de ejecución de EKS](#).

[GuardDuty agrega una nueva funcionalidad – autoEnableOrganizationMembers](#)

23 de marzo de 2023

Amazon GuardDuty agrega una nueva opción de configuración de la organización que ayuda a los administradores de GuardDuty a auditar y hacer cumplir (si es necesario) que GuardDuty esté habilitado para ALL las cuentas de miembro de la organización. La práctica recomendada ahora es utilizar `autoEnableOrganizationMembers` en lugar de `autoEnable`. `autoEnable` está en desuso, pero sigue siendo compatible. Esta nueva funcionalidad afecta a las siguientes API:

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[La característica Protección de RDS en Amazon GuardDuty ya está disponible de forma general](#)

La protección de RDS de GuardDuty supervisa y perfila la actividad de inicio de sesión de RDS para identificar comportamientos de inicio de sesión sospechosos en las instancias de base de datos de Amazon Aurora. Para más información sobre las Regiones de AWS que admiten RDS Protection, consulte [Regiones y puntos de conexión](#).

16 de marzo de 2023

[GuardDuty anuncia la activación de características](#)

Históricamente, la API de GuardDuty permitía configurar tanto las características como los orígenes de datos, pero ahora todos los nuevos tipos de protección de GuardDuty se configurarán como características y no como orígenes de datos. GuardDuty sigue admitiendo los orígenes de datos a través de la API, pero no agregará una nueva API. La activación de características afecta al comportamiento de las API utilizadas para habilitar GuardDuty o un tipo de protección dentro de GuardDuty. Si administra sus cuentas de GuardDuty mediante una plantilla de API, SDK o CFN, consulte [Cambios en la API de GuardDuty en marzo de 2023](#).

16 de marzo de 2023

[Malware Protection for EC2 de GuardDuty ya está disponible en la región Medio Oriente \(EAU\)](#)

La característica de Malware Protection for EC2 en GuardDuty se admite en la región Medio Oriente (EAU). Para obtener más información, consulte [Regiones y puntos de enlace](#).

13 de marzo de 2023

[Amazon GuardDuty ha actualizado el rol vinculado al servicio \(SLR\)](#)

GuardDuty ha agregado los siguientes permisos nuevos para admitir la próxima característica de supervisión en tiempo de ejecución de EKS en GuardDuty.

8 de marzo de 2023

- Utilice las acciones de Amazon EKS para administrar y recuperar información sobre los clústeres de EKS y administrar los complementos de EKS en los clústeres de EKS. Las acciones de EKS también recuperan la información sobre las etiquetas asociadas a GuardDuty.

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"ec2:DescribeVpcEndpointServices",  
"ec2:DescribeSecurityGroups"
```

[Amazon GuardDuty ha actualizado el rol vinculado al servicio \(SLR\)](#)

El rol vinculado al servicio de GuardDuty se ha actualizado para permitir la creación del rol vinculado al servicio de Malware Protection for EC2 después de que se haya habilitado Malware Protection for EC2.

21 de febrero de 2023

GuardDuty requiere TLS v1.2 o posteriores	Para comunicarse con recursos de AWS, GuardDuty requiere y admite TLS v1.2 o posteriores. Para más información, consulte Protección de los datos y Seguridad de la infraestructura .	14 de febrero de 2023
GuardDuty ya está disponible en la región Asia-Pacífico (Hyderabad)	Se ha agregado la región Asia Pacífico (Hyderabad) a la lista de Regiones de AWS en las que GuardDuty está disponible. Para obtener más información, consulte Regiones y puntos de enlace .	14 de febrero de 2023
La guía del usuario de Amazon GuardDuty se alinea con las prácticas recomendadas de IAM	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulta prácticas recomendadas de seguridad en IAM .	10 de febrero de 2023
GuardDuty ya está disponible en la región Europa (España)	Se ha agregado la región Europa (España) a la lista de Regiones de AWS en las que GuardDuty está disponible. Para obtener más información, consulte Regiones y puntos de enlace .	8 de febrero de 2023

[GuardDuty ya está disponible en la región Europa \(Zúrich\)](#)

Se ha agregado la región Europa (Zúrich) a la lista de Regiones de AWS en las que GuardDuty está disponible. Para obtener más información, consulte [Regiones y puntos de enlace](#).

12 de diciembre de 2022

[Versión preliminar de una nueva característica: Protección de RDS con GuardDuty](#)

La protección de RDS de GuardDuty supervisa y perfila la actividad de inicio de sesión de RDS para identificar comportamientos de inicio de sesión sospechosos en las instancias de base de datos de Amazon Aurora. Actualmente, estará disponible para una versión preliminar en cinco Regiones de AWS. Para obtener más información, consulte [Regiones y puntos de enlace](#).

30 de noviembre de 2022

[GuardDuty ya está disponible en la región Medio Oriente \(EAU\)](#)

Se ha agregado la región Medio Oriente (EAU) a la lista de Regiones de AWS en las que GuardDuty está disponible. Para obtener más información, consulte [Regiones y puntos de enlace](#).

6 de octubre de 2022

[Se ha agregado contenido para una nueva característica: Malware Protection for EC2 de GuardDuty2](#)

26 de julio de 2022

Malware Protection for EC2 de GuardDuty es una mejora opcional de Amazon GuardDuty. Mientras GuardDuty identifica los recursos en riesgo, Malware Protection for EC2 detecta el malware que puede ser la razón por la que se han visto comprometidos. Con Malware Protection for EC2 habilitada, siempre que GuardDuty detecte un comportamiento sospechoso en una instancia o carga de trabajo de contenedor de Amazon EC2 indicativo de malware, Malware Protection for EC2 de GuardDuty inicia un análisis sin agente de los volúmenes de EBS asociados a la instancia o a las cargas de trabajo de EC2 afectadas para detectar la presencia de malware. Para obtener información sobre cómo funciona la protección contra Malware para EC2 y la configuración de esta característica, consulte [Malware Protection for EC2 de GuardDuty](#).

- Para obtener información sobre los resultados de Malware Protection for

EC2, consulte [Detalles del resultado](#).

- Para obtener información sobre cómo corregir la instancia y un contenedor independiente de EC2 afectados, consulte [Corrección de problemas de seguridad detectados por GuardDuty](#).
- Para obtener información sobre cómo auditar registros de CloudWatch para análisis de malware y los motivos por los que se omite un recurso durante dicho análisis, consulte [Understanding CloudWatch Logs and skip reasons](#).
- Para obtener información sobre los falsos positivos en las detecciones de amenazas, consulte [Informes de falsos positivos en Malware Protection for EC2 de GuardDuty](#).

[Se ha retirado un tipo de resultado](#)

[Exfiltration:S3/ObjectRead.Unusual](#) Se ha retirado .

5 de julio de 2022

[Se han agregado nuevos tipos de resultados de S3 que identifican comportamientos anómalos mediante el modelo de machine learning \(ML\) con detección de anomalías de GuardDuty.](#)

Se han agregado los siguientes tipos de resultados de S3 nuevos. Estos tipos de resultados identifican si una solicitud de API ha invocado una entidad de IAM de forma anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Para obtener más información sobre cada uno de estos nuevos resultados, consulte [Tipos de resultados de S3](#).

5 de julio de 2022

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[Se ha agregado contenido de protección de EKS con GuardDuty para GuardDuty](#)

GuardDuty ahora puede generar resultados para los recursos de Amazon EKS mediante la supervisión de los registros de auditoría de EKS. Para obtener información sobre cómo configurar esta característica, consulte [Protección de EKS en Amazon GuardDuty](#). Para ver una lista de los resultados que GuardDuty puede generar para los recursos de Amazon EKS, consulte los [resultados de Kubernetes](#). Se ha agregado una nueva guía de corrección para respaldar la corrección de estos resultados en la [Guía de corrección de resultados de Kubernetes](#).

25 de enero de 2022

[Se ha agregado 1 resultado nuevo](#)

Se ha agregado un nuevo resultado UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Este resultado le informa cuando una cuenta de AWS ajena a su entorno de AWS accede a las credenciales de su instancia.

20 de enero de 2022

[Se han actualizado los tipos de resultados para ayudar a identificar los problemas relacionados con log4j](#)

Amazon GuardDuty ha actualizado los siguientes tipos de resultados para ayudar a identificar y priorizar los problemas relacionados con CVE-2021-44228 y CVE-2021-45046: Backdoor: EC2/C&CActivity.B; Backdoor: EC2/C&CActivity.B!DNS; Behavior:EC2/NetworkPortUnusual.

22 de diciembre de 2021

[Cambios en los resultados](#)

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration se ha cambiado por UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Esta versión mejorada del resultado descubre las ubicaciones habituales en las que se utilizan sus credenciales para reducir los resultados del tráfico que se direcciona a través de las redes locales.
[UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)

7 de septiembre de 2021

[Actualización del SLR de GuardDuty](#)

El SLR de GuardDuty se ha actualizado con nuevas acciones para mejorar la precisión de los resultados.

3 de agosto de 2021

[Se ha agregado información sobre el origen de datos de cada tipo de resultado.](#)

Las descripciones de los resultados ahora contienen información sobre los orígenes de datos que GuardDuty utiliza para generar ese resultado.

10 de mayo de 2021

[Se han retirado 13 tipos de resultados.](#)

Se han retirado 13 resultados para sustituirlos por nuevos resultados de Anomalous Behavior. [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](#) y [UnauthorizedAccess:IAMUser/ConsoleLogin](#).

12 de marzo de 2021

[Se han agregado 8 nuevos tipos de resultados para detectar comportamientos anómalos.](#)

Se han agregado 8 nuevos tipos de resultados de IAMUser en función del comportamiento anómalo de las entidades principales de 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 de marzo de 2021

[Se han agregado los resultados de EC2 en función de la reputación del dominio.](#)

Se han agregado 4 nuevos tipos de resultados de impacto en función de la reputación del dominio. [Impact:EC2/AbusedDomainRequest.Reputation](#), [Impact:EC2/BitcoinDomainRequest.Reputation](#), [Impact:EC2/MaliciousDomainRequest.Reputation](#). También se ha agregado un nuevo resultado de EC2 para C&CActivity. [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

27 de enero de 2021

[Se han agregado 4 nuevos tipos de resultados.](#)

Se han agregado 3 nuevos resultados de Malicious IPCaller de S3. [Discovery:S3/MaliciousIPCaller](#), [Exfiltration:S3/MaliciousIPCaller](#), [Impact:S3/MaliciousIPCaller](#). También se ha agregado un nuevo resultado de EC2 para C&CActivity. [Backdoor:EC2/C&CActivity.B](#)

21 de diciembre de 2020

[Se ha retirado el tipo de resultado UnauthorizedAccess:EC2/TorIPCaller.](#)

Ya se ha retirado el tipo de resultado UnauthorizedAccess:EC2/TorIPCaller de GuardDuty. [Más información.](#)

1 de octubre de 2020

[Se ha agregado el tipo de resultado Impact:EC2/WinRmBruteForce.](#)

Se ha agregado un nuevo resultado de impacto, Impact:EC2/WinRmBruteForce. [Más información.](#)

17 de septiembre de 2020

[Se ha agregado el tipo de resultado Impact:EC2/PortSweep.](#)

Se ha agregado un nuevo resultado de impacto, Impact:EC2/PortSweep. [Más información.](#)

17 de septiembre de 2020

[GuardDuty ya está disponible en las regiones África \(Ciudad del Cabo\) y Europa \(Milán\).](#)

Se han agregado África (Ciudad del Cabo) y Europa (Milán) a la lista de regiones de AWS en las que está disponible GuardDuty. [Más información](#)

31 de julio de 2020

Se han agregado nuevos detalles de uso para supervisar los costos de GuardDuty.

Ahora puede usar nuevas métricas para consultar los datos de costos de uso de GuardDuty para su cuenta y las cuentas que administra. Encontrará nueva información general sobre los costos de uso en la consola, en <https://console.aws.amazon.com/guardduty/>. Se puede acceder a información más detallada a través de la API.

31 de julio de 2020

Se ha agregado contenido que cubre la protección de S3 mediante la supervisión de eventos de datos de S3 en GuardDuty.

La protección de S3 de GuardDuty ya está disponible mediante la supervisión de eventos del plano de datos de S3 como un nuevo origen de datos. Las cuentas nuevas tendrán esta característica habilitada automáticamente. Si ya utiliza GuardDuty, puede habilitar el nuevo origen de datos para usted o sus cuentas de miembros.

31 de julio de 2020

Se han agregado 14 resultados de S3 nuevos.

Se han agregado 14 nuevos tipos de resultados de S3 para los orígenes del plano de control y del plano de datos de S3.

31 de julio de 2020

[Se ha agregado compatibilidad adicional para los resultados de S3 y se han cambiado 2 nombres de tipos de resultados existentes.](#)

Los resultados de GuardDuty ahora incluyen más detalles para los resultados relacionados con buckets de S3. Se ha cambiado el nombre de los tipos de resultados existentes que estaban relacionados con la actividad de S3: Policy:IAMUser/S3BlockPublicAccessDisabled se ha cambiado a Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled se ha cambiado a Stealth:S3/ServerAccessLoggingDisabled.

28 de mayo de 2020

[Se ha agregado contenido para la integración de AWS Organizations.](#)

GuardDuty ahora está integrado con los administradores delegados de AWS Organizations, lo que permite administrar cuentas de GuardDuty dentro de la organización. Cuando se establece un administrador delegado como cuenta de administrador de GuardDuty, se puede habilitar automáticamente GuardDuty para que la cuenta de administrador delegado administre a cualquier miembro de la organización. También puede habilitar GuardDuty automáticamente en las nuevas cuentas de miembro de AWS Organizations. [Más información.](#)

20 de abril de 2020

[Se ha agregado contenido para la característica Exportar los resultados.](#)

Se ha agregado contenido que describe la característica Exportar los resultados de GuardDuty.

14 de noviembre de 2019

[Se ha agregado el tipo de resultado UnauthorizedAccess:EC2/MetadataDNSRebind.](#)

Se ha agregado un nuevo resultado no autorizado, UnauthorizedAccess:EC2/MetadataDNSRebind. [Más información.](#)

10 de octubre de 2019

Se ha agregado el tipo de resultado Stealth:IAMUser/S3ServerAccessLoggingDisabled.	Se ha agregado un nuevo resultado invisible, Stealth:IAMUser/S3ServerAccessLoggingDisabled. Más información.	10 de octubre de 2019
Se ha agregado el tipo de resultado Policy:IAMUser/S3BlockPublicAccessDisabled.	Se ha agregado un nuevo resultado de política, Policy:IAMUser/S3BlockPublicAccessDisabled. Más información.	10 de octubre de 2019
Se ha retirado el tipo de resultado Backdoor:EC2/XORDDOS.	Se ha retirado el tipo de resultado Backdoor:EC2/XORDDOS de GuardDuty. Más información	12 de junio de 2019
Se ha agregado el tipo de resultado PrivilegeEscalation.	El tipo de resultado Privilege Escalation detecta cuando los usuarios intentan asignar privilegios escalados y más permisivos a sus cuentas. Más información	14 de mayo de 2019
GuardDuty ya está disponible en la región Europa (Estocolmo).	Se ha agregado la región Europa (Estocolmo) a la lista de regiones de AWS en las que está disponible GuardDuty. Más información	9 de mayo de 2019
Se ha agregado un nuevo tipo de resultado, Recon:EC2/PortProbeEMRUnprotectedPort.	Este resultado le informa de que un puerto sensible relacionado con ERM en una instancia EC2 no está bloqueado y se está sondeando activamente. Más información	8 de mayo de 2019

[Se han agregado 5 tipos de resultados nuevos que detectan si las instancias de EC2 se están utilizando posiblemente para llevar a cabo ataques de denegación de servicio \(DoS\).](#)

Estos resultados le informan de las instancias EC2 de su entorno cuyo comportamiento puede indicar que se están utilizando para llevar a cabo ataques de denegación de servicio (DoS). [Más información](#)

8 de marzo de 2019

[Se ha agregado un nuevo tipo de resultado: Policy:IAMUser/RootCredentialUsage](#)

El tipo de resultado Policy:IAMUser/RootCredentialUsage le informa de que las credenciales de inicio de sesión del usuario raíz de la Cuenta de AWS se están utilizando para hacer solicitudes a los servicios de AWS mediante programación. [Más información](#)

24 de enero de 2019

[UnauthorizedAccess:IAMUser/UnusualASNCaller Se ha retirado el tipo de resultado](#)

Se ha retirado el tipo de resultado UnauthorizedAccess:IAMUser/UnusualASNCaller. Ahora, se utilizarán otros tipos de resultados de GuardDuty activos para informarle de cualquier actividad que se invoque desde redes poco habituales. El tipo de resultado generado dependerá de la categoría de la API que se invocó desde una red inusual. [Más información](#)

21 de diciembre de 2018

[Se han agregado dos nuevos tipos de resultados: PenTest:IAMUser/ParrotLinux y PenTest:IAMUser/PentooLinux](#)

El tipo de resultado PenTest:IAMUser/ParrotLinux le informa de que un equipo que ejecuta Parrot Security Linux está haciendo llamadas a la API con las credenciales que pertenecen a su cuenta de AWS. El tipo de resultado PenTest:IAMUser/PentooLinux le informa de que una máquina que ejecuta Pentoo Linux está haciendo llamadas a la API con las credenciales que pertenecen a su cuenta de AWS. [Más información](#)

21 de diciembre de 2018

[Se ha agregado compatibilidad con el tema de SNS de anuncios de Amazon GuardDuty](#)

Ahora se puede suscribir al tema de SNS de anuncios de GuardDuty para recibir notificaciones sobre nuevos tipos de resultados publicados, actualizaciones para los tipos de resultados existentes u otros cambios en funcionalidades. Las notificaciones están disponibles en todos los formatos que admite Amazon SNS. [Más información](#)

21 de noviembre de 2018

[Se han agregado dos nuevos tipos de resultados: UnauthorizedAccess:EC2/TorClient y UnauthorizedAccess:EC2/TorRelay](#)

El tipo de resultado UnauthorizedAccess:EC2/TorClient le informa de que una instancia de EC2 de su entorno de AWS está llevando a cabo conexiones a un nodo Authority o Guard de Tor. El tipo de resultado UnauthorizedAccess:EC2/TorRelay le informa de que una instancia de EC2 de su entorno de AWS está llevando a cabo conexiones a una red de Tor, lo que sugiere que actúa como un relé de Tor. [Más información](#)

16 de noviembre de 2018

[Se ha agregado un nuevo tipo de resultado: Cryptocurrency:EC2/BitcoinTool.B](#)

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que está consultando un nombre de dominio que está asociado con actividad relacionada con Bitcoin u otras criptomonedas. [Más información](#)

9 de noviembre de 2018

[Se ha agregado compatibilidad con la actualización de la frecuencia de notificaciones enviadas a Eventos de CloudWatch](#)

Ahora puede actualizar la frecuencia de las notificaciones enviadas a CloudWatch Events de las apariciones posteriores de resultados ya obtenidos. Los valores posibles son 15 minutos, una hora o seis horas, que es el valor predeterminado. [Más información](#)

9 de octubre de 2018

<u>Se han agregado regiones compatibles</u>	Se ha agregado compatibilidad con la región AWS GovCloud (Oeste de EE. UU.). <u>Más información</u>	25 de julio de 2018
<u>Se ha agregado compatibilidad con CloudFormation StackSets en GuardDuty</u>	Puede utilizar la plantilla Enable Amazon GuardDuty (Habilitar Amazon GuardDuty) para habilitar este servicio simultáneamente en varias cuentas. <u>Más información</u>	25 de junio de 2018
<u>Se ha agregado compatibilidad con las reglas de archivado automático de GuardDuty</u>	Los clientes ya pueden crear reglas de archivado automático o detalladas para la supresión de resultados. En el caso de los resultados que coinciden con una regla de archivado automático, GuardDuty los marca automáticamente como archivados. Esto permite a los clientes configurar GuardDuty para que solo conserve los resultados de la tabla de resultados actual. <u>Más información</u>	4 de mayo de 2018
<u>GuardDuty está disponible en la región Europa (París)</u>	GuardDuty ya está disponible en la región Europa (París), lo que le permite ampliar el servicio de supervisión de seguridad y detección de amenazas continuo en esta región. <u>Más información</u>	29 de marzo de 2018

[Ahora se admite la creación de cuentas de administrador de GuardDuty y cuentas de miembro a través de CloudFormation.](#)

Para obtener más información, consulte [AWS::GuardDuty::master](#) y [AWS::GuardDuty::member](#).

6 de marzo de 2018

[Se han agregado nuevas detecciones de anomalías basadas en CloudTrail.](#)

Estos nuevos tipos de resultados se habilitan automáticamente en GuardDuty en todas las regiones compatibles. [Más información](#)

28 de febrero de 2018

[Se han agregado nuevas detecciones de inteligencia de amenazas \(tipos de resultados\).](#)

Estos nuevos tipos de resultados se habilitan automáticamente en GuardDuty en todas las regiones compatibles. [Más información](#)

5 de febrero de 2018

[Incremento del límite de cuentas de miembro de GuardDuty.](#)

Con esta versión, puede tener hasta 1000 cuentas de miembro de GuardDuty agregadas por cada cuenta de AWS (cuenta de administrador de GuardDuty). [Más información](#)

25 de enero de 2018

[Cambios en la carga y posterior administración de listas de IP de confianza y listas de amenazas para la cuenta de administrador de GuardDuty y las cuentas de miembro.](#)

Con esta versión, los usuarios de cuentas de administrador de GuardDuty pueden cargar y administrar listas de IP de confianza y listas de amenazas. Los usuarios de cuentas de miembro de GuardDuty no pueden cargar ni administrar listas. Las listas de IP de confianza y las listas de amenazas que son cargadas por la cuenta del administrador son impuestas a la funcionalidad de GuardDuty en sus cuentas de miembro.

[Más información](#)

25 de enero de 2018

Actualizaciones anteriores

Cambio	Descripción	Fecha
Publicación inicial	Publicación inicial de la Guía del usuario de Amazon GuardDuty.	28 de noviembre de 2017